

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**REISSUE PATENT APPLICATION TRANSMITTAL**

Address to:  <b>Mail Stop Reissue Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450</b>	Attorney Docket No.	ARAC-01RE1
	First Named Inventor	Rozman, Allen F.
	Original Patent Number	7,484,247 B2
	Original Patent Issue Date (Month/Day/Year)	Jan. 27,2009
	Express Mail Label No.	

**APPLICATION FOR REISSUE OF:**  
(Check applicable box)

Utility Patent



Design Patent



Plant Patent

**APPLICATION ELEMENTS (37 CFR 1.173)**

1.  Fee Transmittal Form (PTO/SB/56)
2.  Applicant claims small entity status. See 37 CFR 1.27.
3.  Specification and Claims in double column copy of patent format  
(amended, if appropriate)
4.  Drawing(s) (proposed amendments, if appropriate)
5.  Reissue Oath/Declaration (original or copy)  
(37 C.F.R. 1.175) (PTO/SB/51 or 52)
6.  Power of Attorney
7.  Original U.S. Patent currently assigned?  Yes  No  
(If Yes, check applicable box(es))  
 Written Consent of all Assignees (PTO/SB/53)  
 37 CFR 3.73(b) Statement (PTO/SB/96)
8.  CD-ROM or CD-R in duplicate, Computer Program (Appendix)  
or large table  
 Landscape Table on CD
9. Nucleotide and/or Amino Acid Sequence Submission  
(if applicable, items a. – c. are required))
  - a.  Computer Readable Form (CRF)
  - b. Specification Sequence Listing on:
    - i.  CD-ROM (2 copies) or CD-R (2 copies); or
    - ii.  paper
  - c.  Statements verifying identity of above copies

**ACCOMPANYING APPLICATION PARTS**

10.  Statement of status and support for all  
changes to the claims. See 37 CFR 1.173(c).
11.  Foreign Priority Claim (35 U.S.C. 119)  
(if applicable)
12.  Information Disclosure Statement (IDS)  
PTO/SB/08 or PTO-1449  
 Copies of citations attached
13.  English Translation of Reissue Oath/Declaration  
(if applicable)
14.  Preliminary Amendment
15.  Return Receipt Postcard (MPEP 503)  
(Should be specifically itemized)
16.  Other:

**17. CORRESPONDENCE ADDRESS**
 The address associated with Customer Number:  OR  Correspondence address below

Name	Allen F. Rozman				
Address	6402 Wildlife Trail				
City	Garland	State	TX	Zip Code	75044
Country	USA	Telephone	214-478-2172	Email	arozman@verizon.net
Signature	/A. F. Rozman/			Date	3/9/2010
Name (Print/Type)	Allen F. Rozman		Registration No. (Attorney/Agent)	41280	

This collection of information is required by 37 CFR 1.173. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Mail Stop Reissue, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

## Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>REISSUE APPLICATION: CONSENT OF ASSIGNEE; STATEMENT OF NON-ASSIGNMENT</b>		Docket Number (Optional)  ARAC-01RE1
This is part of the application for a reissue patent based on the original patent identified below.		
Name of Patentee(s) Rozman; Allen F,                      Cioffi; Alfonso J		
Patent Number 7,484,247	Date Patent Issued January 27, 2009	
Title of Invention System and method for protecting a computer system from malicious software.		
<p>1. <input type="checkbox"/> Filed herein is a statement under 37 CFR 3.73(b). (Form PTO/SB/96)</p> <p>2. <input checked="" type="checkbox"/> Ownership of the patent is in the inventor(s), and no assignment of the patent is in effect.</p> <p>One of boxes 1 or 2 above must be checked. If multiple assignees, complete this form for each assignee. If box 2 is checked, skip the next entry and go directly to "Name of Assignee".</p> <p>The written consent of all assignees and inventors owning an undivided interest in the original patent is included in this application for reissue.</p> <p>The assignee(s) owning an undivided interest in said original patent is/are _____, and the assignee(s) consents to the accompanying application for reissue.</p>		
Name of assignee/inventor (if not assigned) Rozman; Allen F,    Cioffi; Alfonso J		
Signature 		Date 3-9-10
Typed or printed name and title of person signing for assignee (if assigned)		

This collection of information is required by 37 CFR 1.172. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

## Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicants: Rozman, *et al.*                      Docket No.: ARAC-01RE1  
Serial No.: TBD                                      Filed: Herewith  
Reissue of: 7,484,247                              Issued: January 27, 2009  
Title: System and Method for Protecting a Computer System from Malicious Software.

Mail Stop: REISSUE  
Commissioner for Patents  
P. O. Box 1450  
Alexandria, VA 22313-1450

**PRELIMINARY AMENDMENT**

Dear Sir:

Prior to examination on the merits, Applicants respectfully submit the amendments and remarks set forth below.

In the Specification:

Before the heading “Cross Reference to Related Patents and Applications” please insert:

Cross Reference to Multiple Reissue Applications

This application is a reissue application of U.S. Patent No. 7,484,247, entitled “System and Method for Protecting a Computer System from Malicious Software,” issued on January 27, 2009, and is related to another reissue application designated U.S. Patent Application Serial No. \_\_\_\_\_ (Docket No. ARAC-01RE2) from U.S. Patent No. 7,484,247 filed concurrently herewith, which are incorporated herein by reference.

Claims (1, 2, 6, 10, 11, 15, 17 and 20) are currently amended from their form in U.S. Patent No. 7,484,247. Claims (3, 4, 5, 7, 8, 9, 12, 13, 14, 16, 18 and 19) are in their original form in U.S. Patent No. 7,484,247.

1) (Currently amended) A method of operating a computer system capable of exchanging data across a network of one or more computers and having at least a first and second electronic data processor capable of executing instructions using a common operating system, comprising the steps of:

executing browser instructions in a first logical process within the common operating system using the first electronic data processor, wherein the first logical process is capable of accessing data contained in a first memory space ~~and a second memory space;~~

executing instructions in a second logical process within the common operating system using the second electronic data processor, wherein the second logical process is capable of accessing data contained in the second memory space, ~~the second logical process being further capable of exchanging data across a network of one or more computers;~~

displaying, ~~in a windowed format on a display terminal,~~ data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to [the] a display terminal;

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is

20 protected from corruption by a malware process downloaded from the network and  
21 executing as part of the second logical process.

1 2) (Currently amended) The method of claim 1 wherein the ~~first memory space and the~~  
2 second memory space ~~comprise separate regions of a common memory space~~ is selected  
3 from the group consisting of:

4 a memory zone within a physical memory common to the first memory space;

5 a partition on a memory device;

6 random access memory (RAM);

7 both volatile and nonvolatile memory.

1 3) (Original) The method of claim 1 wherein the second logical process is selected from the  
2 group consisting of:

3 an electronic mail process, an instant messaging process, an internet browser process,  
4 an interactive gaming process, a virtual private network (VPN) process, and a reader  
5 application process.

1 4) (Original) The method of claim 1 wherein the first logical process receives user interface  
2 data, and passes the user interface data to the second logical process.

1 5) (Original) The method of claim 1 wherein the first and second electronic data processors  
2 are part of a multi-core electronic data processor.

1 6) (Currently amended) The method of claim 1 and further comprising the step of restoring  
2 at least one corrupted data file ~~residing on the second memory space~~ from [an] a  
3 protected image ~~residing on the first memory space~~.

1 7) (Original) The method of claim 1 and further comprising the step of automatically  
2 deleting at least one data file residing on the second memory space when the second  
3 logical process is terminated.

1 8) (Original) The method of claim 1 and further comprising the steps of:  
2 encrypting data with the first logical process;  
3 transferring the encrypted data from the first logical process to the second logical  
4 process;  
5 transferring the encrypted data from the second logical process to the network  
6 interface device.

1 9) (Original) The method of claim 8 and further comprising the steps of:  
2 decrypting the data with the network interface device;  
3 transferring the decrypted data from the network interface device to the network

1 10) (Currently amended) A multi-processor computer system using a common operating  
2 system capable of exchanging data across a network of one or more computers via a  
3 network interface device, comprising:  
4 a first electronic data processor capable of executing browser instructions using the  
5 common operating system and communicatively coupled to a first memory space ~~and a~~

6 ~~second memory space;~~

7 a second electronic data processor capable of executing browser instructions using  
8 the common operating system and communicatively coupled to [the] a second memory  
9 ~~space and to a network interface device, wherein the second electronic data processor is~~  
10 ~~capable of exchanging data across a network of one or more computers via the network~~  
11 ~~interface device;~~

12 a video processor adapted to combine video data from the first and second electronic  
13 data processors and transmit the combined video data to a display ~~terminal for displaying~~  
14 ~~the combined video data in a windowed format;~~

15 wherein the computer system is configured such that the second electronic data  
16 processor is operating in a protected mode and data residing on the first memory space is  
17 protected from corruption by a malware process downloaded from the network and  
18 executing on the second electronic data processor.

1 11) (Currently amended) The computer system of claim 10 wherein the ~~first memory space~~  
2 ~~and the second memory space comprise separate regions of a common memory space is~~  
3 selected from the group consisting of:

4 a memory zone within a physical memory common to the first memory space;

5 a partition on a memory device;

6 random access memory (RAM);

7 both volatile and nonvolatile memory.

1 12) (Original) The computer system of claim 10 wherein the first and second electronic data  
2 processors are part of a dual processor computer system.

1 13) (Original) The computer system of claim 10 wherein the second electronic data  
2 processor and the video processor are co-located on a circuit card, the circuit card being  
3 communicatively coupled to the first electronic data processor.

1 14) (Original) The computer system of claim 10 wherein the computer system is configured  
2 such that the first electronic data processor is protected from executing instructions  
3 initiated by a malware process downloaded from the network and executing on the  
4 second electronic data processor.

1 15) (Currently amended) A multi-processor computer system using a common operating  
2 system capable of exchanging data across a network of one or more computers,  
3 comprising:

4 at least a first and second electronic data processor capable of executing instructions  
5 using the common operating system;

6 at least a first and second memory space;

7 a video processor;

8 wherein the first and second electronic data processors, first and second memory  
9 space, and video processor are configured for performing the steps of;

10 executing browser instructions in a first logical process with the first electronic data  
11 processor, wherein the first logical process is executing within the common operating  
12 system and is capable of accessing data contained in the first memory space ~~and the~~  
13 ~~second memory space~~;

14 executing browser instructions in a second logical process with the second electronic  
15 data processor, wherein the second logical process is executing within the common

16 operating system and is capable of accessing data contained in the second memory space;  
17 ~~the second logical process being further capable of exchanging data across a network of~~  
18 ~~one or more computers;~~

19 displaying, ~~in a windowed format on a display terminal,~~ data from the first logical  
20 process and the second logical process, wherein the video processor is adapted to  
21 combine data from the first and second logical processes and transmit the combined data  
22 to [the] a display terminal;

23 wherein the computer system is configured such that the second electronic data  
24 processor is operating in a protected mode and data residing on the first memory space is  
25 protected from corruption by a malware process downloaded from the network and  
26 executing as part of the second logical process.

1 16) (Original) The computer system of claim 15 wherein the computer system is further  
2 configured such that the first logical process is protected from executing instructions  
3 initiated by a malware process downloaded from the network and executing as part of the  
4 second logical process.

1 17) (Currently amended) The computer system of claim 15 and further comprising: at least  
2 one network interface device capable of exchanging data with ~~both the second logical~~  
3 ~~process and with~~ the network and with a logical process selected from the group  
4 consisting of:

5 the first logical process;  
6 the second logical process.



1 18) (Original) The computer system of claim 17 wherein the network interface device is  
2 capable of decrypting data received from the second logical process and transmitting the  
3 decrypted data to the network while preventing the second logical process from accessing  
4 the decrypted data.

1 19) (Original) The computer system of claim 15 wherein the at least one electronic data  
2 processor is selected from the group consisting of: a multi-core electronic data processor;  
3 dual electronic data processors; and multiple electronic data processors.

1 20) (Currently amended) The computer system of claim 15 and further configured for  
2 performing the step of: restoring at least one corrupted data file ~~residing on the second~~  
3 ~~memory space~~ from [an] a protected image ~~residing on the first memory space~~.

Please add the following new claims (21-57)

1 21) (New) A portable computer, comprising:

2 a network interface device configured to exchange data across a network of one or  
3 more computers using a wireless connection;

4 at least a first memory space and a second memory space, the first memory space  
5 containing at least one system file;

6 at least one electronic data processor communicatively coupled to the network  
7 interface device, the first and second memory space, and to a user interface, wherein the  
8 user interface is configured to receive input from a computer user;

9 the at least one electronic data processor configured to execute a first browser process  
10 in a first logical process, wherein the first logical process is capable of accessing data  
11 contained in the first memory space;

12 the at least one electronic data processor further configured to execute a second  
13 browser process in a second logical process, wherein the second logical process is  
14 capable of accessing data contained in the second memory space and is further capable of  
15 generating video data;

16 a video processor configured to transmit video data from the second browser process  
17 to a display;

18 wherein the first browser process is capable of opening the second browser process  
19 and is further capable of passing data to the second browser process;

20 wherein further the portable computer is configured such that the at least one system

21 file residing on the first memory space is protected from corruption by a malware process  
22 downloaded from the network and executing within the second browser process.

1 22) (New) The portable computer of Claim 21 wherein the first browser process is capable  
2 of exchanging data with the network interface device and with the second browser  
3 process.

1 23) (New) The portable computer of Claim 22 wherein the first browser process is capable of  
2 passing data downloaded from the network to the second browser process.

1 24) (New) The portable computer of Claim 21 wherein the second browser process is capable  
2 of exchanging data with the network interface device and with the first browser process.

1 25) (New) The portable wireless communication device of Claim 21 wherein the at least one  
2 electronic data processor is selected from the group consisting of:

3 an Application Specific Integrated Circuit;

4 a Field Programmable Gate Array;

5 a plurality of electronic data processors;

6 a multi-core electronic data processor.

1 26) (New) The portable computer of Claim 21 wherein the second memory space is selected  
2 from the group consisting of:

3 a memory zone within a physical memory common to the first memory space;

4 a partition on a memory device;

5 random access memory (RAM);  
6 both volatile and nonvolatile memory.

1 27) (New) The portable computer of Claim 21 configured such that at least one corrupted file  
2 required for a browser process is capable of being restored from a protected image.

1 28) (New) The portable computer of Claim 27 wherein the protected image is stored at a  
2 location selected from the group consisting of:

- 3 a removable drive;
- 4 the first memory space;
- 5 a partition on a memory device;
- 6 a nonvolatile memory disk;
- 7 another device.

1 29) (New) The portable computer of Claim 21 configured such that at least one corrupted file  
2 residing on the second memory space is capable of being automatically deleted when the  
3 second browser process is terminated.

1 30) (New) The portable computer of Claim 21 configured such that the first browser process  
2 is protected from executing instructions initiated by a malware process downloaded from  
3 the network and executing as part of the second browser process.

1 31) (New) The portable computer of Claim 21 wherein attempts by malware to record data  
2 entry by the computer user are effectively blocked.

1 32) (New) A method of operating a portable computer having at least one electronic data  
2 processor communicatively coupled to a first and second memory space and to a network  
3 interface device, wherein the network interface device is configured to exchange data  
4 across a network of one or more computers using a wireless connection, comprising the  
5 steps of:

6 storing at least one system file within the first memory space;

7 executing a first browser process in a first logical process using the at least one  
8 electronic data processor, wherein the first logical process is configured to access data  
9 contained in the first memory space;

10 executing a second browser process in a second logical process using the at least  
11 one electronic data processor, wherein the second logical process is configured to access  
12 data contained in the second memory space and is further configured to generate video  
13 data;

14 opening the second browser process on instruction from the first browser process;

15 passing data from the first browser process to the second browser process;

16 displaying video data from the second browser process;

17 wherein the portable computer is configured such that the at least one system file  
18 residing on the first memory space is protected from corruption by a malware process  
19 downloaded from the network and executing as part of the second browser process.

1 33) (New) The method of Claim 32 wherein the portable computer is configured such that the  
2 first browser process is capable of exchanging data with the network interface device and  
3 with the second browser process.

1 34) T(New) The method of Claim 33 and further comprising the step of;  
2 downloading data from the network and passing the data from the first browser  
3 process to the second browser process.

1 35) (New) The method of Claim 32 wherein the portable computer is configured such that the  
2 second browser process is capable of exchanging data with the network interface device  
3 and with the first browser process.

1 36) (New) The method of Claim 32 wherein the second memory space is selected from the  
2 group consisting of:  
3 a memory zone within a physical memory common to the first memory space;  
4 a partition on a memory device;  
5 random access memory (RAM);  
6 both volatile and nonvolatile memory.

1 37) (New) The method of Claim 32 and further comprising the step of;  
2 restoring at least one corrupted file from a protected image.

1 38) (New) The method of Claim 37 wherein the protected image is stored at a location  
2 selected from the group consisting of:  
3 a removable drive;  
4 the first memory space;  
5 a partition on a memory device;

6 a nonvolatile memory disk;  
7 another device.

1 39) (New) The method of Claim 32 and further comprising the step of;  
2 deleting at least one corrupted data file residing on the second memory space  
3 when the second logical process is terminated.

1 40) (New) The method of Claim 32 wherein the at least one electronic data processor is  
2 selected from the group consisting of:  
3 an Application Specific Integrated Circuit;  
4 a Field Programmable Gate Array;  
5 a plurality of electronic data processors;  
6 a multi-core electronic data processor.

1 41) (New) The method of Claim 32 wherein the first browser process is protected from  
2 executing instructions initiated by a malware process downloaded from the network and  
3 executing as part of the second browser process.

1 42) (New) The method of Claim 32 and further comprising the step of:  
2 displaying video data from the first browser process.

1 43) (New) The method of Claim 32 wherein attempts by malware to record data entry by the  
2 computer user are effectively blocked.

1 44) (New) A portable computer, comprising:  
2 a network interface device configured to exchange data across a network of one or  
3 more computers using a wireless connection;  
4 at least a first memory space and a second memory space;  
5 at least one electronic data processor communicatively coupled to the network  
6 interface device, the first and second memory space, and to a user interface, wherein the  
7 user interface is configured to receive input from a computer user;  
8 wherein the portable computer is configured for performing the steps of:  
9 storing at least one system file in the first memory space;  
10 opening a first browser process, wherein the first browser process is capable of  
11 accessing data contained in the first memory space;  
12 opening a second browser process, wherein the second browser process is capable  
13 of accessing data contained in the second memory space, and is further capable of  
14 generating video data;  
15 passing data from the first browser process to the second browser process;  
16 displaying video data from the second browser process;  
17 wherein the portable computer is configured such that the at least one system file  
18 residing on the first memory space is protected from corruption by a malware process  
19 downloaded from the network and executing as part of the second browser process.

1 45) (New) The portable computer of Claim 44 wherein the first browser process is capable of  
2 exchanging data with the network interface device and with the second browser process.



1 46) (New) The portable computer of Claim 45 and further configured for performing the step  
2 of:  
3 downloading data from the network and passing the downloaded data from the  
4 first browser process to the second browser process.

1 47) (New) The portable computer of Claim 46 and further configured for performing the step  
2 of:  
3 storing the downloaded data on the second memory space.

1 48) (New) The portable computer of Claim 44 wherein the second browser process is capable  
2 of exchanging data with the network interface device and with the first browser process.

1 49) (New) The portable computer of Claim 44 and further configured for performing the step  
2 of:  
3 restoring at least one corrupted file from a protected image.

1 50) (New) The portable computer of Claim 49 wherein the protected image is stored at a  
2 location selected from the group consisting of:  
3 a removable drive;  
4 the first memory space  
5 a partition on a memory device;  
6 a non-volatile memory disk;  
7 another device.

1 51) (New) The portable computer of Claim 44 configured such that at least one corrupted file  
2 residing on the second memory space is capable of being automatically deleted when the  
3 second browser process is terminated.

1 52) (New) The portable computer of Claim 44 wherein the first browser process is protected  
2 from executing instructions initiated by a malware process downloaded from the network  
3 and executing as part of the second browser process.

1 53) (New) The portable computer of Claim 44 and further configured for performing the step  
2 of:  
3 the first browser process instructing the second browser process to open.

1 54) (New) The portable computer of Claim 44 wherein attempts by malware to record data  
2 entry by the computer user are effectively blocked.

1 55) (New) The portable computer of Claim 44 wherein the at least one electronic data  
2 processor is selected from the group consisting of:  
3 an Application Specific Integrated Circuit;  
4 a Field Programmable Gate Array;  
5 a plurality of electronic data processors;  
6 a multi-core electronic data processor.

1 56) (New) The portable computer of Claim 44 wherein the second memory space is selected  
2 from the group consisting of:  
3 a memory zone within a physical memory common to the first memory space;

4 a partition on a memory device;  
5 random access memory (RAM);  
6 both volatile and nonvolatile memory.

1 57) (New) The portable computer of Claim 44 and further configured for performing the step  
2 of:  
3 the first browser process opening a plurality of second browser processes.

## REMARKS

The Applicants respectfully provide the following remarks related to the claim amendments submitted above. Claims (1, 2, 6, 10, 11, 15, 17 and 20) are currently amended from their form in U.S. Patent No. 7,484,247. Claims (3, 4, 5, 7, 8, 9, 12, 13, 14, 16, 18 and 19) are in their original form in U.S. Patent No. 7,484,247. Claims 21-57 have been added (new) by this Preliminary Amendment. Applicants respectfully provide notice that more than one reissue application has been filed on U.S. Patent No. 7,484,247, as required under 37 C.F.R. § 1.177(a).

Claims 21-57 have been added to more comprehensively claim the subject invention. No new subject matter has been added by the claims, and the new claims are fully supported in the specification, as demonstrated in the attached Appendix entitled Status of Claims and Support for Claim Changes, as required under 37 C.F.R. § 1.173(c). The support shown in the Appendix is by way of example only and the Applicants make no representation that the identified support is the only or best support for the claims. Other support than that specifically cited in the Appendix may be found in the specification, drawings, and original claims, as well.

Please enter the above amendments before consideration of this application. The Applicants believe the claims are in condition for allowance and respectfully request that the Examiner pass the case to reissuance. The Examiner is invited to contact the undersigned to address any questions or concerns regarding the present reissue application.

Respectfully submitted,

\_\_\_\_\_  
3/9/2010  
Date

\_\_\_\_\_  
/A. F. Rozman/  
Allen F. Rozman  
Co-Applicant  
Registered Patent Agent  
Reg. No. 41,280

**APPENDIX**

**STATUS OF CLAIMS AND  
SUPPORT FOR CLAIM CHANGES**

<b>Claims</b>	<b>Status</b>	<b>Support</b>		
1	Currently amended	Col 9 lines 30-37 Fig. 1, 190, 195	Col 11 lines 2-4 Fig. 1, 120, 191, 190, 110, 130	
2	Currently amended	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
3	Original			
4	Original			
5	Original			
6	Currently amended	Fig. 4, 420	Col 12 lines 46-58	
7	Original			
8	Original			
9	Original			
10	Currently amended	Col 9 lines 30-37 Fig. 1, 190, 195	Col 11 lines 2-4 Fig. 1, 120, 191, 190, 110, 130	
11	Currently amended	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
12	Original			
13	Original			
14	Original			
15	Currently amended	Col 9 lines 30-37 Fig. 1, 190, 195	Col 11 lines 2-4 Fig. 1, 120, 191, 190, 110, 130	
16	Original			
17	Currently amended	Fig. 1, 120, 191, 190, 110, 130		
18	Original			
19	Original			
20	Currently amended	Fig. 4, 420	Col 12 lines 46-58	
21	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53 Fig. 1, 120, 191, 190, 110, 130	Fig. 1, 120, 150, 160 Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Col 11 lines 2-4 Col 8 lines 1-6	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 23-28
22	New	Fig. 1, 120, 191, 190		

23	New	Fig. 1, 120, 191, 190, 195	Col 11 lines 38-41	
24	New	Fig. 1, 140, 190		
25	New	Col 14 lines 62-67	Col 9 lines 30-47	
26	New	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
27	New	Fig. 4, 420	Col 12 lines 46-58	
28	New	Col 12 lines 46-58	Col 7 lines 13-16	
29	New	Col 8 lines 23-26		
30	New	Col 19 lines 33-37		
31	New	Col 7 lines 58-62		
32	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Col 11 lines 2-4 Col 8 lines 1-6	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 23-28
33	New	Fig. 1, 120, 191, 190		
34	New	Fig. 1, 120, 191, 190, 195	Col 11 lines 38-41	
35	New	Fig. 1, 140, 190		
36	New	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
37	New	Fig. 4, 420	Col 12 lines 46-58	
38	New	Col 12 lines 46-58	Col 7 lines 13-16	
39	New	Col 8 lines 23-26		
40	New	Col 14 lines 62-67	Col 9 lines 30-47	
41	New	Col 19 lines 33-37		
42	New	Fig. 1, 120, 170, 171, 180		
43	New	Col 7 lines 58-62		
44	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Col 11 lines 2-4 Col 8 lines 1-6	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 25-28
45	New	Fig. 1, 120, 191, 190		
46	New	Fig. 1, 120, 191, 190, 195	Col 11 lines 38-41	
47	New	Fig. 3, 320		
48	New	Fig. 1, 140, 190		
49	New	Fig. 4, 420	Col 12 lines 46-58	
50	New	Col 12 lines 46-58	Col 7 lines 13-16	

51	New	Col 8 lines 23-26		
52	New	Col 19 lines 33-37		
53	New	Fig 2. 220		
54	New	Col 7 lines 58-62		
55	New	Col 14 lines 62-67	Col 9 lines 30-47	
56	New	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
57	New	Col 13 lines 22-24	Fig 2, 220	

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>				
<b>Filing Date:</b>				
<b>Title of Invention:</b>	System and Method for Protecting a Computer System from Malicious Software			
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman			
<b>Filer:</b>	Glenn W. Boisbrun/Jill Errera			
<b>Attorney Docket Number:</b>	ARAC-01RE1			
Filed as Small Entity				
<b>Reissue (Utility) Filing Fees</b>				
<b>Description</b>	<b>Fee Code</b>	<b>Quantity</b>	<b>Amount</b>	<b>Sub-Total in USD(\$)</b>
<b>Basic Filing:</b>				
Utility Reissue Basic	2014	1	165	165
Design and utility Reissue Basic	2114	1	270	270
Design and utility Reissue Basic	2314	1	325	325
<b>Pages:</b>				
<b>Claims:</b>				
Reissue claims in excess of 20 for small	2205	37	26	962
Independent claims reissue small	2204	3	110	330
<b>Miscellaneous-Filing:</b>				



Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				
<b>Miscellaneous:</b>				
			<b>Total in USD (\$)</b>	<b>2052</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	7171049
<b>Application Number:</b>	12720147
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	8473
<b>Title of Invention:</b>	System and Method for Protecting a Computer System from Malicious Software
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Correspondence Address:</b>	Allen F. Rozman - 6402 Wildlife Trail - Garland TX 75044 US 214-478-2172 arozman@verizon.net
<b>Filer:</b>	Glenn W. Boisbrun/Jill Errera
<b>Filer Authorized By:</b>	Glenn W. Boisbrun
<b>Attorney Docket Number:</b>	ARAC-01RE1
<b>Receipt Date:</b>	09-MAR-2010
<b>Filing Date:</b>	
<b>Time Stamp:</b>	14:52:00
<b>Application Type:</b>	Reissue (Utility)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$2052

RAM confirmation Number		1260			
Deposit Account					
Authorized User					
<b>File Listing:</b>					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		US_Pat_7484247.pdf	834434	yes	23
			5443fa976291dd744ca4d8b7622293e252c607d0		
	<b>Multipart Description/PDF files in .zip description</b>				
	<b>Document Description</b>		<b>Start</b>	<b>End</b>	
	Specification		1	2	
	Drawings-only black and white line drawings		3	13	
	Specification		14	23	
<b>Warnings:</b>					
<b>Information:</b>					
2	Oath or Declaration filed	ARAC-01RE1_sb0051.pdf	1230805	no	3
			95c6959d8cc12083b9ffb6131f16e82c54a0760c		
<b>Warnings:</b>					
<b>Information:</b>					
3	Transmittal Reissue Application	ARAC-01RE1_sb0050.pdf	205193	no	2
			00d425e3b0c45b83f0988886de76522babd6ce4		
<b>Warnings:</b>					
<b>Information:</b>					
4	Consent of Assignee accompanying the declaration.	ARAC-01RE1_sb0053.pdf	994168	no	2
			f3fd015e4920476281f38c455de61c6bc716a3db		
<b>Warnings:</b>					
<b>Information:</b>					
5		ARAC-01RE1_Preliminary_Amendment_1.pdf	60419	yes	23
			092fb4fd850caaf5057ee3ea41f4d3d5d867fb84		
	<b>Multipart Description/PDF files in .zip description</b>				
	<b>Document Description</b>		<b>Start</b>	<b>End</b>	
	Preliminary Amendment		1	1	
	Specification		2	2	

	Claims	3	19
	Applicant Arguments/Remarks Made in an Amendment	20	23

**Warnings:**

**Information:**

6	Fee Worksheet (PTO-875)	fee-info.pdf	37995	no	2
			8461c0ac16e4b426d0b9e77ead2ea5a71aa23a9e		

**Warnings:**

**Information:**

<b>Total Files Size (in bytes):</b>		3363014
-------------------------------------	--	---------

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**



US007484247B2

(12) **United States Patent**  
**Rozman et al.**

(10) **Patent No.:** **US 7,484,247 B2**  
(45) **Date of Patent:** **Jan. 27, 2009**

(54) **SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE**

(76) Inventors: **Allen F Rozman**, 735 Mockingbird Dr., Murphy, TX (US) 75094; **Alfonso J Cioffi**, 719 Mockingbird Dr., Murphy, TX (US) 75094

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 710 days.

5,978,917 A	11/1999	Chi	
5,995,103 A	11/1999	Ashe	
6,134,661 A	10/2000	Topp	
6,167,522 A	12/2000	Lee et al.	
6,192,477 B1 *	2/2001	Corthell	726/11
6,199,181 B1	3/2001	Rechef et al.	
6,216,112 B1	4/2001	Fuller et al.	
6,275,938 B1	8/2001	Bond et al.	
6,351,816 B1	2/2002	Mueller et al.	
6,385,721 B1 *	5/2002	Puckette	713/2
6,480,198 B2	11/2002	Kang	
6,507,904 B1	1/2003	Ellison et al.	

(Continued)

(21) Appl. No.: **10/913,609**

(22) Filed: **Aug. 7, 2004**

(65) **Prior Publication Data**  
US 2006/0031940 A1 Feb. 9, 2006

(51) **Int. Cl.**  
**G06F 1/26** (2006.01)  
**G06F 12/14** (2006.01)  
**G06F 11/30** (2006.01)  
**H04L 9/32** (2006.01)

(52) **U.S. Cl.** ..... **726/34; 713/192; 713/193**

(58) **Field of Classification Search** ..... None  
See application file for complete search history.

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

4,890,098 A	12/1989	Dawes et al.	
5,280,579 A	1/1994	Nye	
5,502,808 A	3/1996	Goddard et al.	
5,555,364 A	9/1996	Goldstein	
5,666,030 A	9/1997	Parson	
5,673,403 A *	9/1997	Brown et al.	715/744
5,751,979 A	5/1998	McCrary	
5,826,013 A	10/1998	Nachenberg	
5,918,039 A	6/1999	Buswell et al.	

**OTHER PUBLICATIONS**

Kevin Townsend; "Spyware, Adware, and Peer to Peer Networks; The Hidden Threat to Corporate Security" © Pest Patrol, 2003.

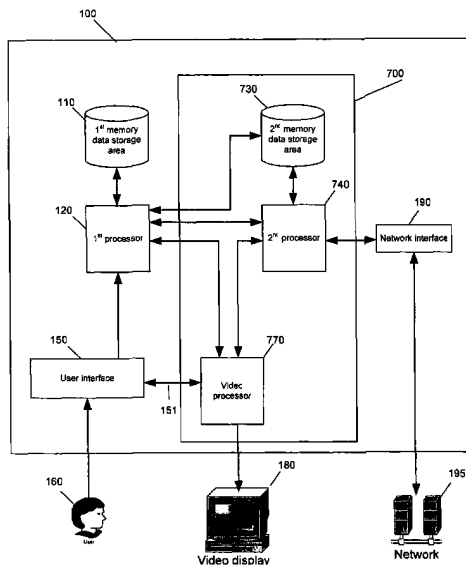
(Continued)

*Primary Examiner*—Christian LaForgia  
(74) *Attorney, Agent, or Firm*—Allen F Rozman

(57) **ABSTRACT**

In a computer system, a first electronic data processor is communicatively coupled to a first memory space and a second memory space. A second electronic data processor is communicatively coupled the second memory space and to a network interface device. The second electronic data processor is capable of exchanging data across a network of one or more computers via the network interface device. A video processor is adapted to combine video data from the first and second electronic data processors and transmit the combined video data to a display terminal for displaying the combined video data in a windowed format. The computer system is configured such that a malware program downloaded from the network and executing on the second electronic data processor is incapable of initiating access to the first memory space.

**20 Claims, 11 Drawing Sheets**



U.S. PATENT DOCUMENTS

6,507,948 B1\* 1/2003 Curtis et al. .... 717/174  
 6,546,554 B1 4/2003 Schmidt et al.  
 6,553,377 B1 4/2003 Eschelbeck et al.  
 6,578,140 B1 6/2003 Policard  
 6,581,162 B1 6/2003 Angelo et al.  
 6,633,963 B1 10/2003 Ellison et al.  
 6,658,573 B1 12/2003 Bischof et al.  
 6,663,000 B1 12/2003 Muttik et al.  
 6,678,712 B1\* 1/2004 McLaren et al. .... 718/100  
 6,678,825 B1 1/2004 Ellison et al.  
 6,735,700 B1 5/2004 Flint et al.  
 7,146,640 B2\* 12/2006 Goodman et al. .... 726/16  
 7,260,839 B2\* 8/2007 Karasaki ..... 726/11  
 2002/0066016 A1 5/2002 Riordan  
 2002/0174349 A1 11/2002 Wolff et al.  
 2003/0023857 A1 1/2003 James et al.

2003/0097591 A1 5/2003 Phan et al.  
 2003/0177397 A1 9/2003 Samman  
 2004/0006715 A1 1/2004 Skrepetos  
 2004/0034794 A1 2/2004 Mayer et al.  
 2004/0039944 A1\* 2/2004 Karasaki ..... 713/201  
 2004/0054588 A1 3/2004 Jacobs et al.  
 2005/0240810 A1\* 10/2005 Safford et al. .... 714/10  
 2006/0004667 A1\* 1/2006 Neil ..... 705/59

OTHER PUBLICATIONS

David Stang, PhD; "Beyond Viruses: Why Anti-Virus Software is No Longer Enough", © Pest Patrol 2002.  
 "The Web: Threat or Menace?" From "Firewalls and Internet Security: Repelling the Wiley Hacker", Second Edition, Addison-Wesley, ISBN 0-201-63466-X, 2003 ©.

\* cited by examiner

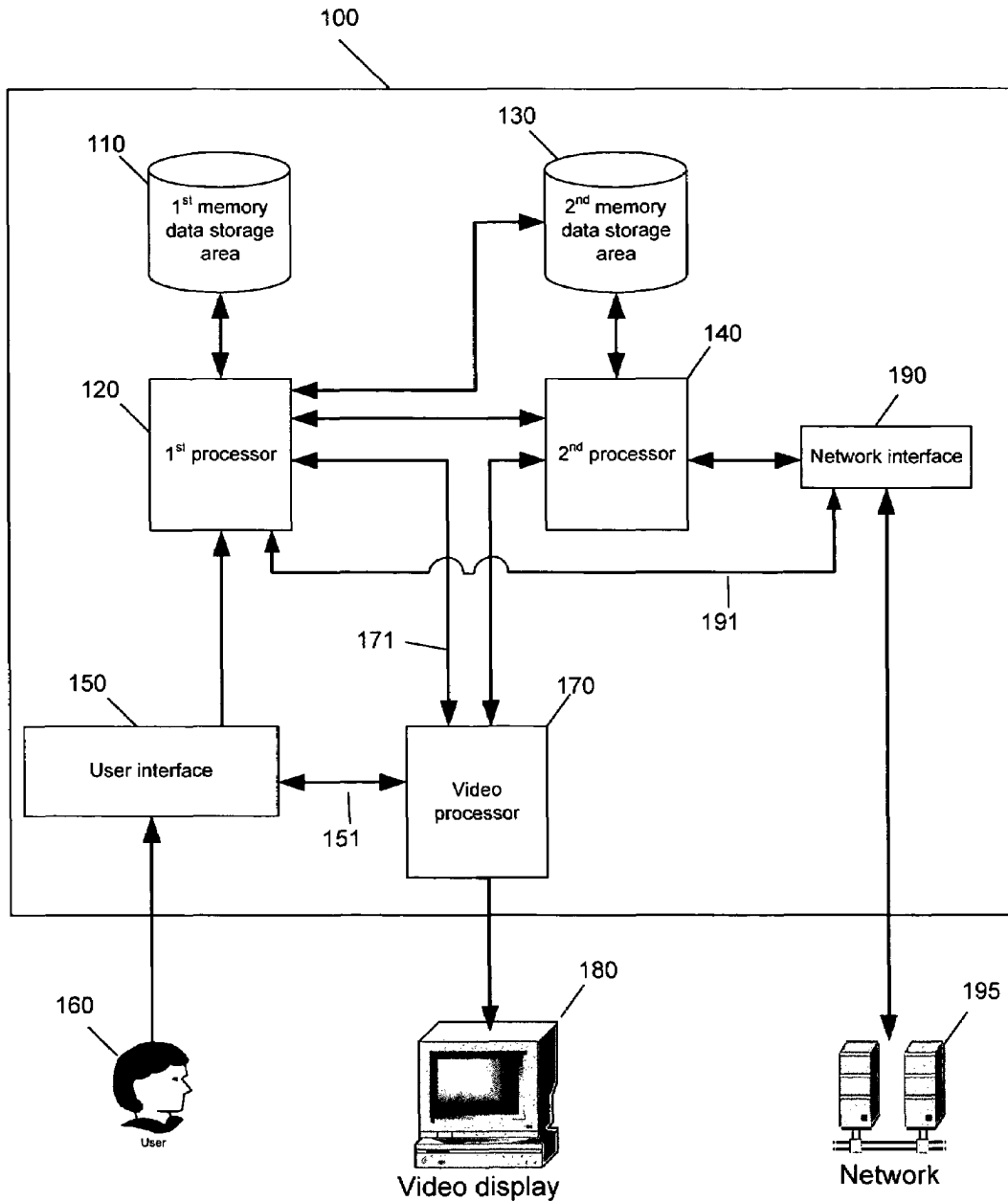


Fig. 1

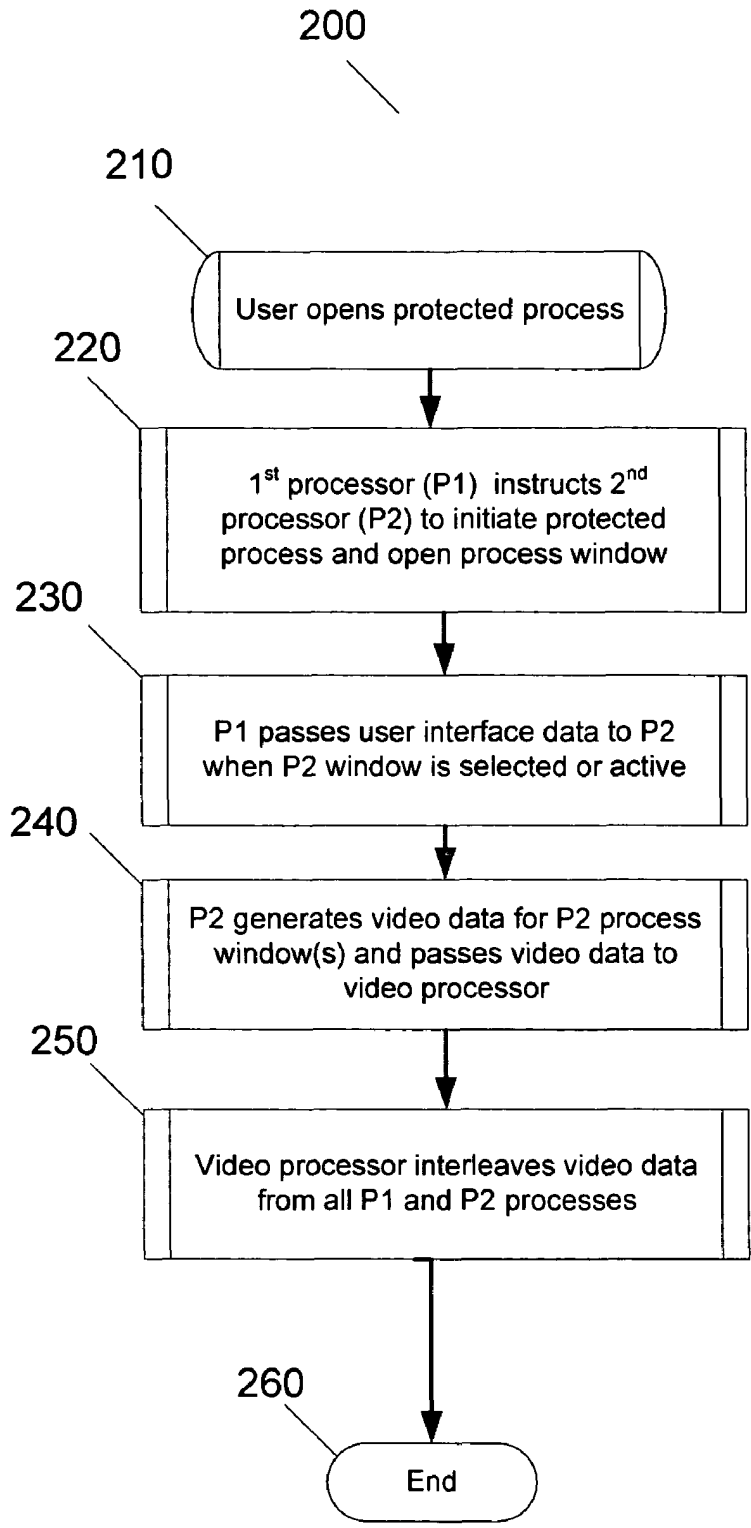


Fig. 2



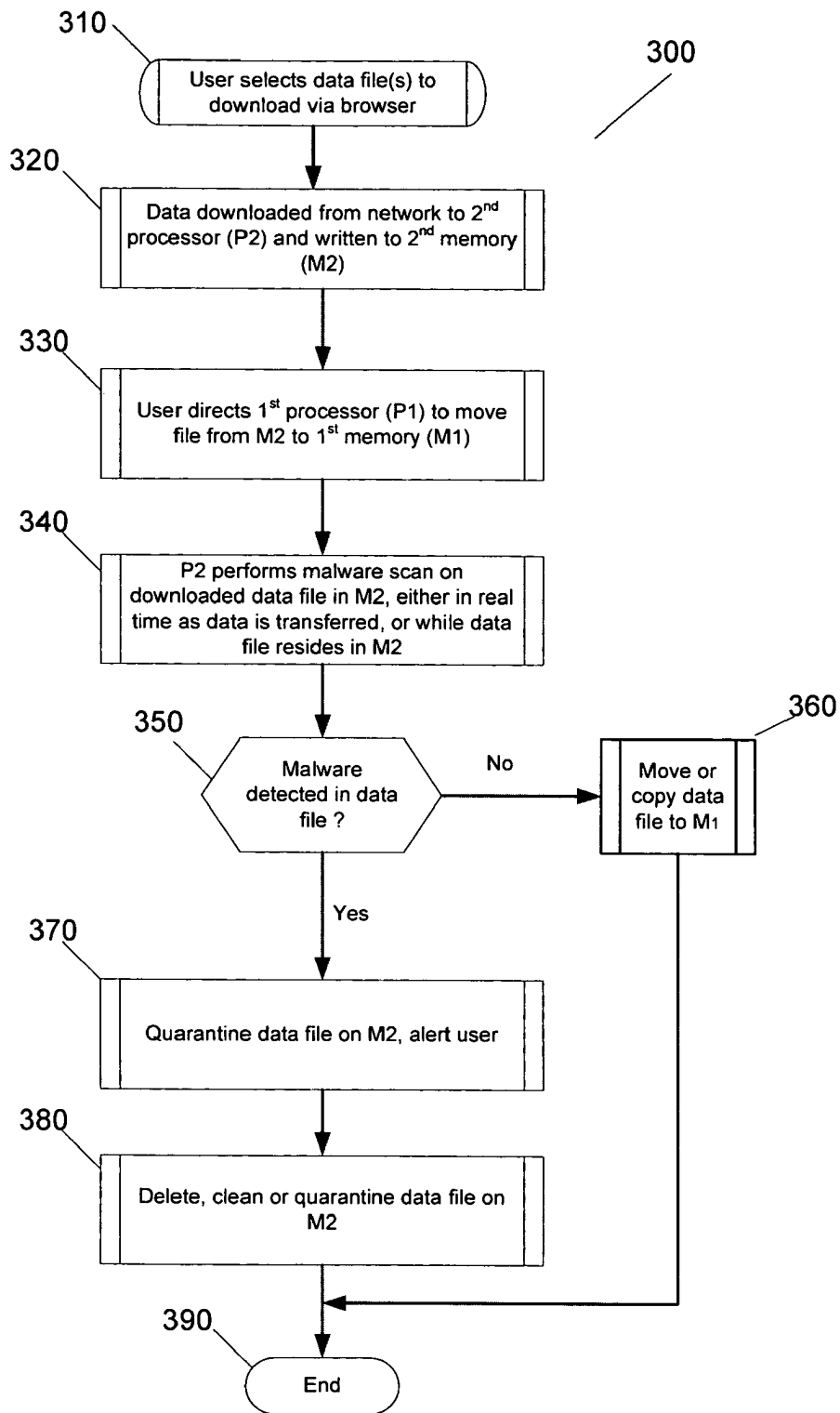


Fig. 3

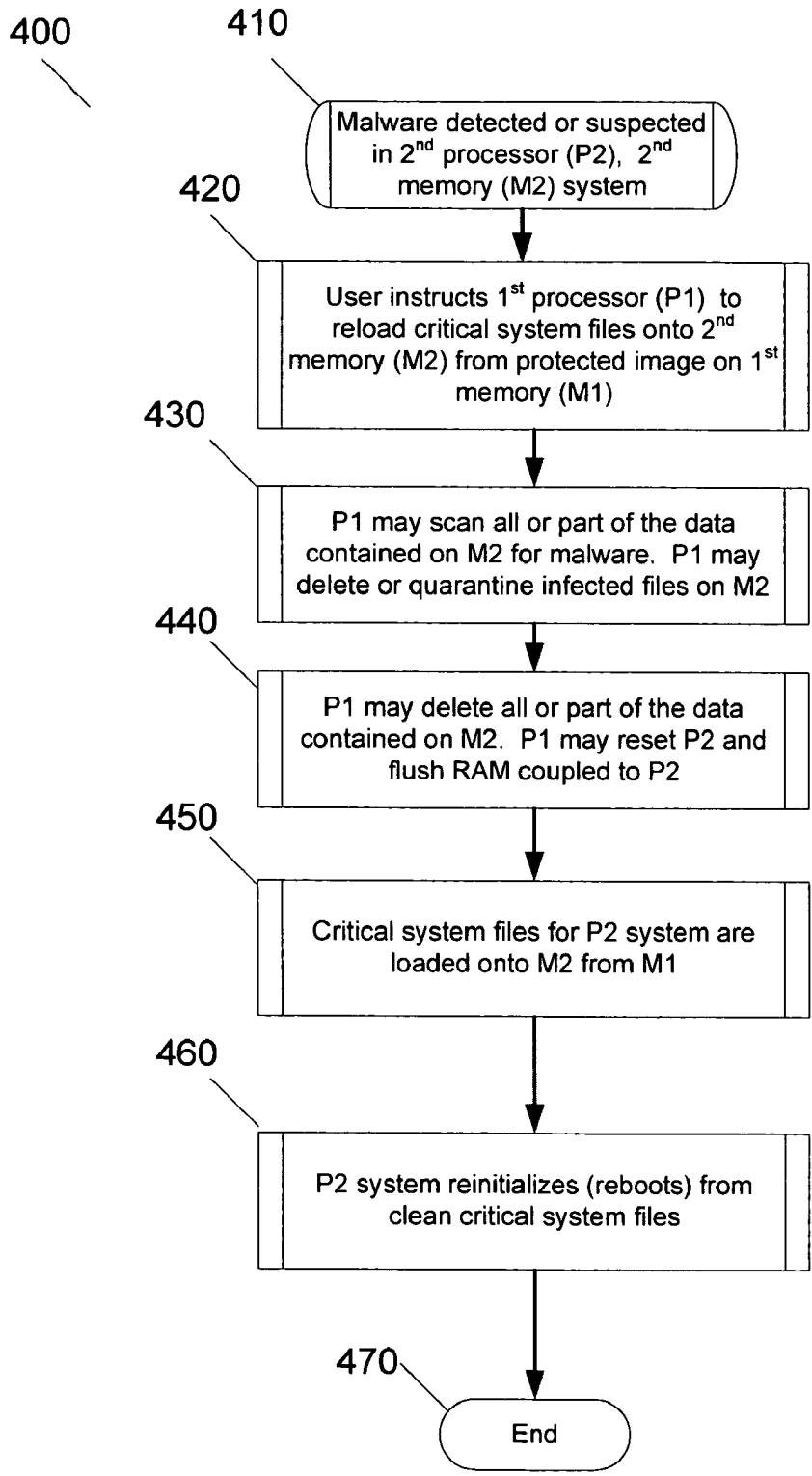


Fig. 4

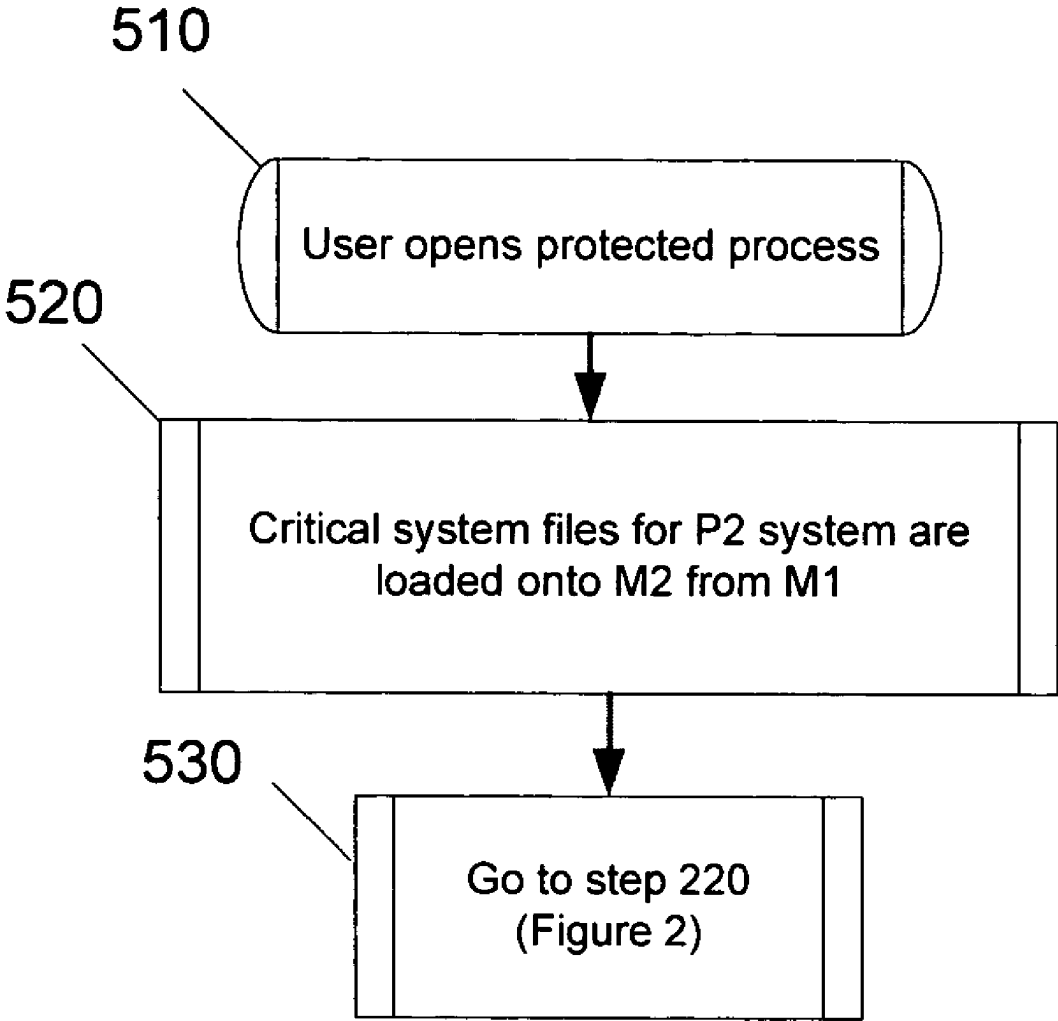


Fig. 5A

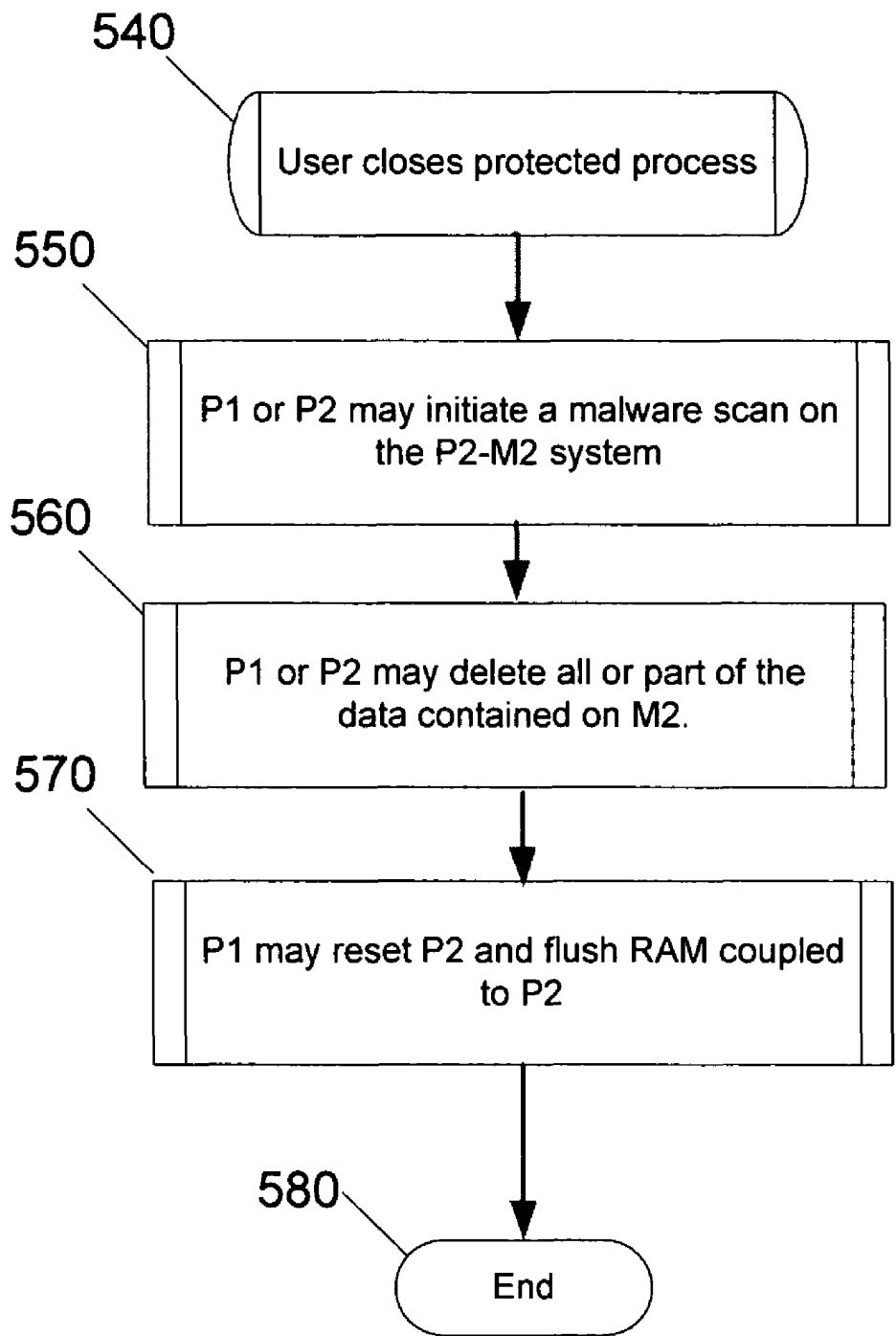


Fig. 5B

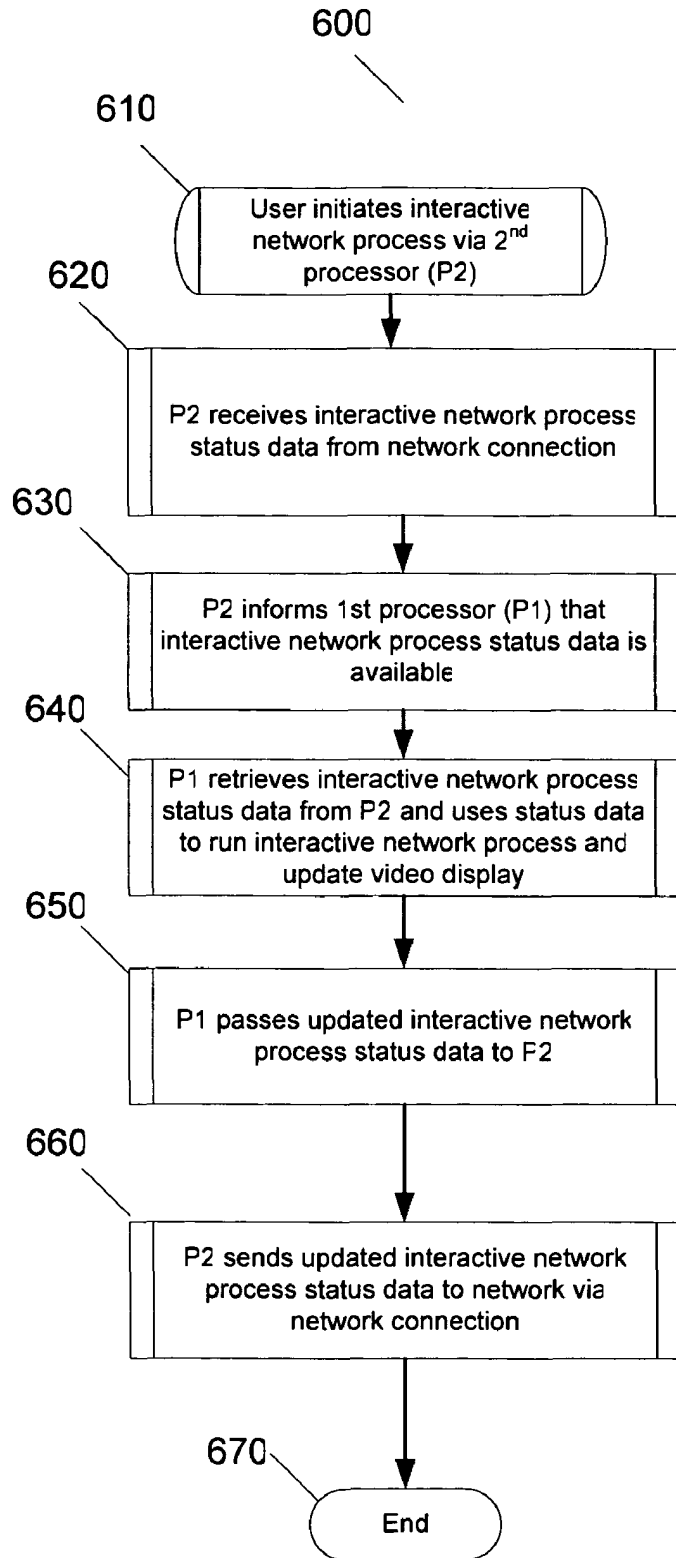


Fig. 6

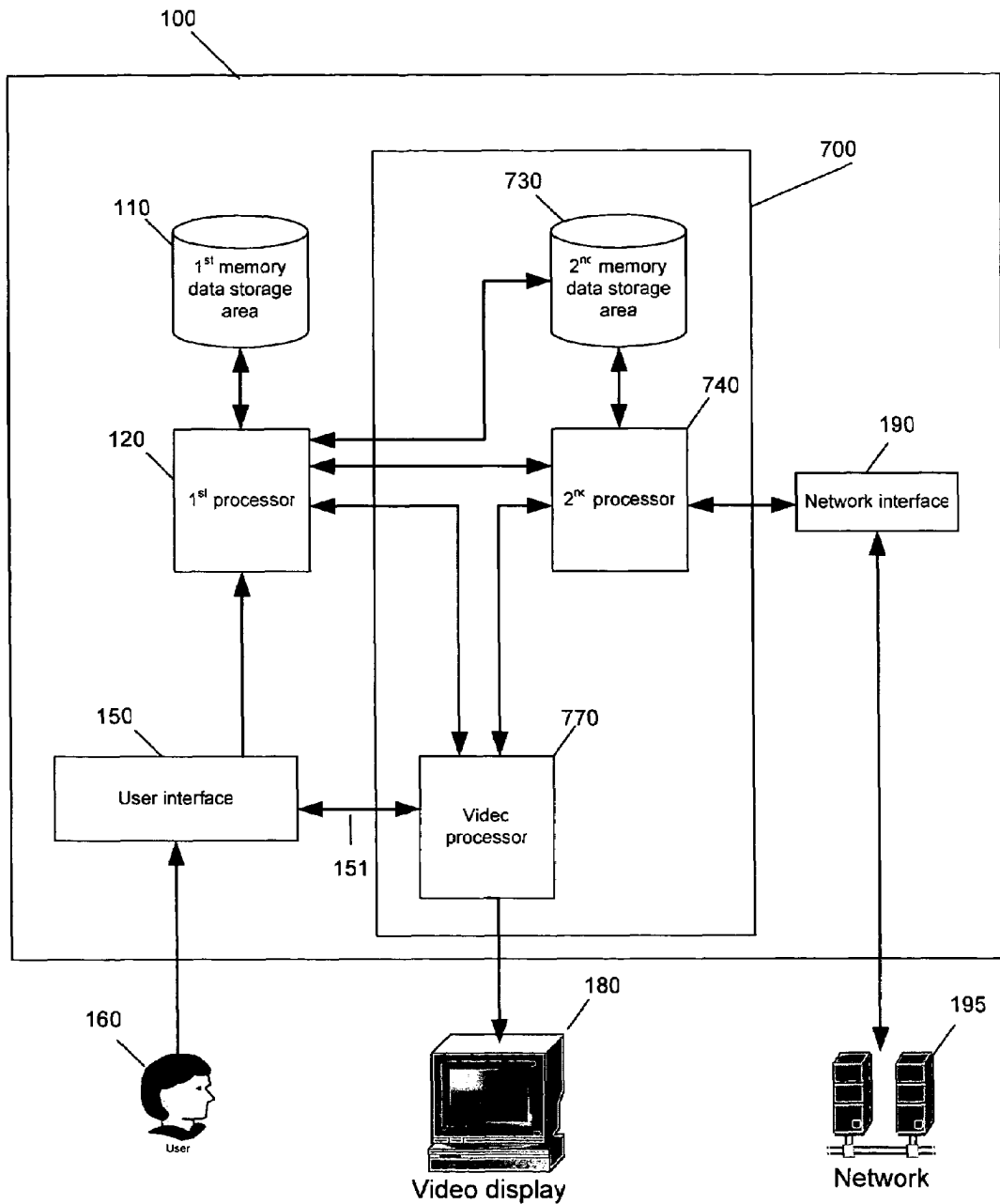


Fig. 7

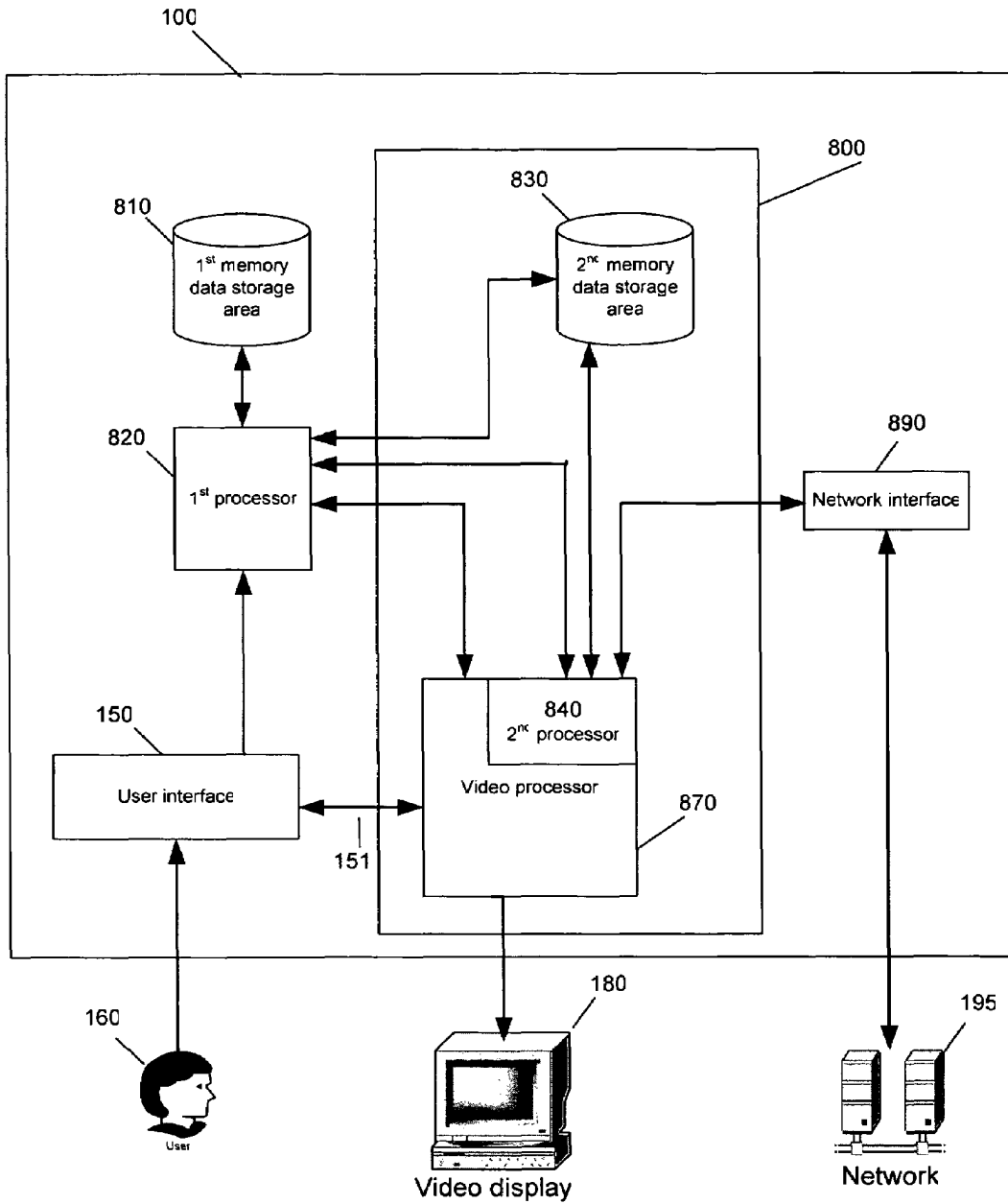


Fig 8

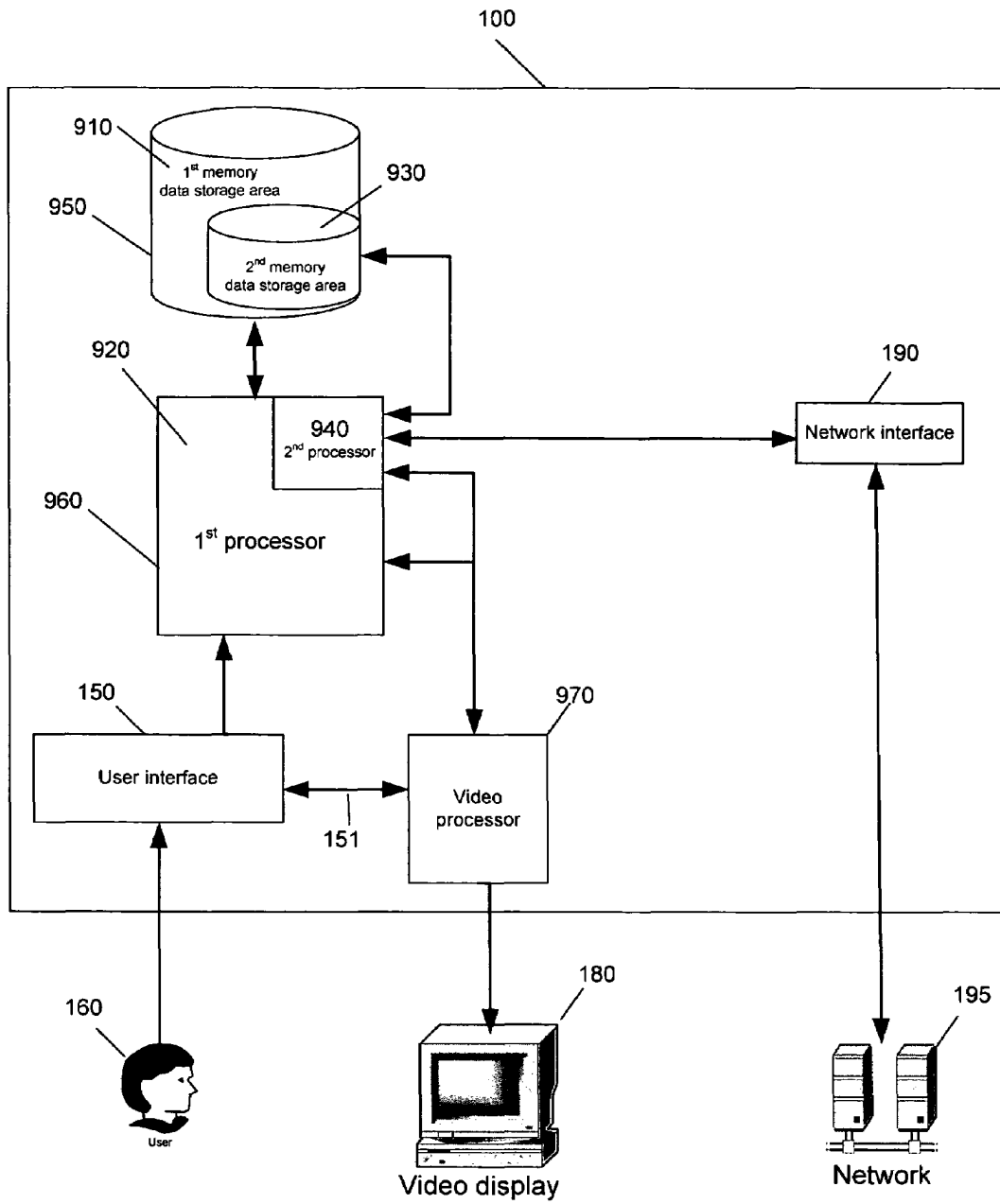


Fig. 9



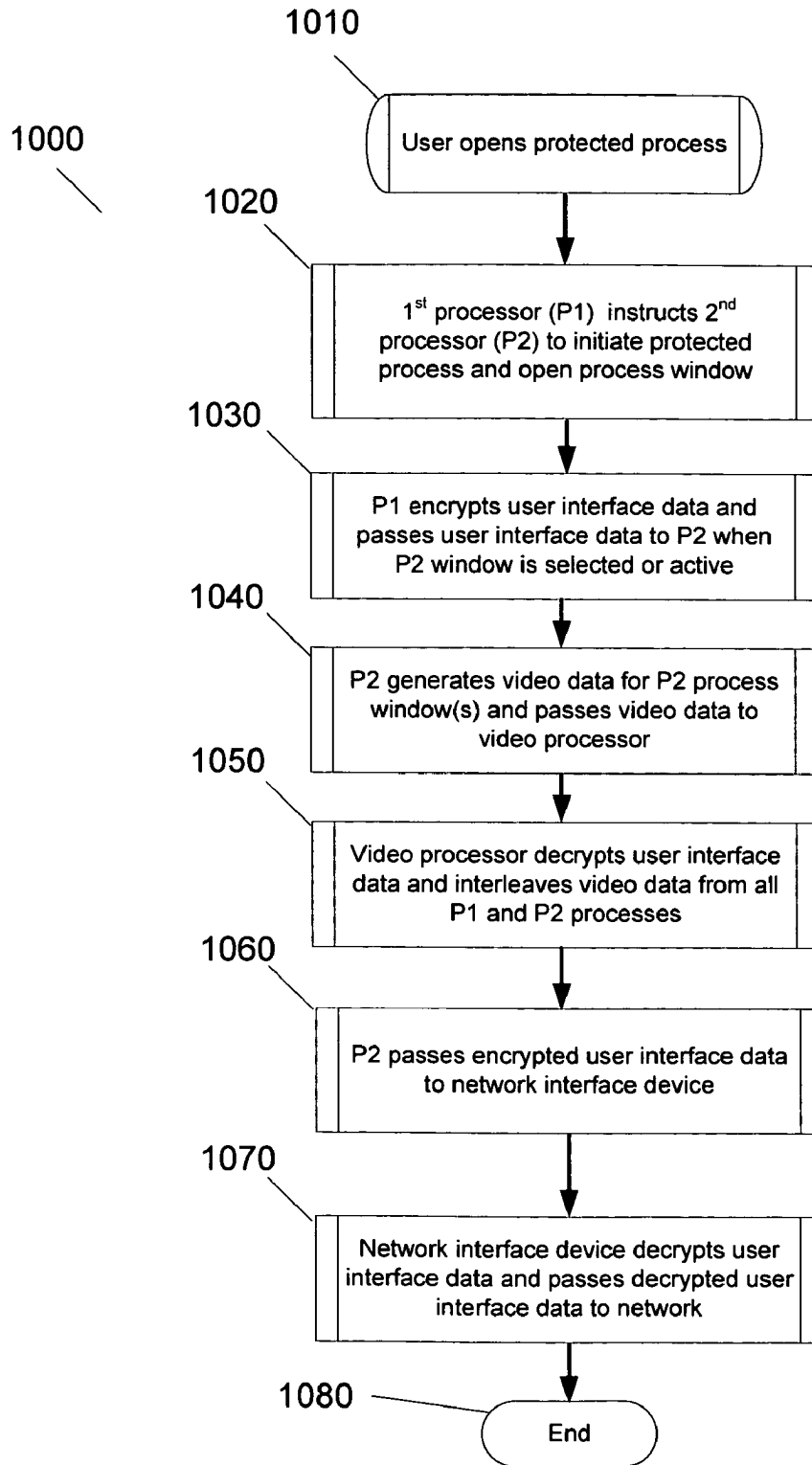


Fig. 10

1

**SYSTEM AND METHOD FOR PROTECTING  
A COMPUTER SYSTEM FROM MALICIOUS  
SOFTWARE**

## TECHNICAL FIELD

The present invention relates generally to computer hardware and software, and more particularly to a system and

2

method for protecting a computer system from malicious software.

CROSS REFERENCE TO RELATED PATENTS  
AND APPLICATIONS

5

This application is related to the following U.S. patents and applications:

U.S. patent or PUB Application Number	Title	Inventor(s)
5,826,013	Polymorphic virus detection module.	Nachenberg
5,978,917	Detection and elimination of macro viruses.	Chi
6,735,700	Fast virus scanning using session stamping.	Flint, et al
6,663,000	Validating components of a malware scanner.	Muttik, et al.
6,553,377	System and process for maintaining a plurality of remote security applications using a modular framework in a distributed computing environment.	Eschelbeck, et al.
6,216,112	Method for software distribution and compensation with replenishable advertisements.	Fuller, et al.
4,890,098	Flexible window management on a computer display.	Dawes, et al.
5,555,364	Windowed computer display.	Goldstein
5,666,030	Multiple window generation in computer display.	Parson
5,995,103	Window grouping mechanism for creating, manipulating and displaying windows and window groups on a display screen of a computer system.	Ashe
5,502,808	Video graphics display system with adapter for display management based upon plural memory sources.	Goddard, et al.
5,280,579	Memory mapped interface between host computer and graphics system.	Nye
5,918,039	Method and apparatus for display of windowing application programs on a terminal.	Buswell, et al
6,480,198	Multi-function controller and method for a computer graphics display system.	Kang
6,167,522	Method and apparatus for providing security for servers executing application programs received via a network	Lee, et al.
6,199,181	Method and system for maintaining restricted operating environments for application programs or operating systems.	Rechef, et al.
6,275,938	Security enhancement for untrusted executable code.	Bond, et al.
6,321,337	Method and system for protecting operations of trusted internal networks.	Reshef, et al.
6,351,816	System and method for securing a program's execution in a network environment.	Mueller, et al.
6,546,554	Browser-independent and automatic apparatus and method for receiving, installing and launching applications from a browser on a client computer.	Schmidt, et al.
6,658,573	Protecting resources in a distributed computer system.	Bischof, et al
6,507,904	Executing isolated mode instructions in a secure system running in privilege rings.	Ellison, et al.
6,633,963	Controlling access to multiple memory zones in an isolated execution environment.	Ellison, et al.
6,678,825	Controlling access to multiple isolated memories in an isolated execution environment.	Ellison, et al.
5,751,979	Video hardware for protected, multiprocessing systems.	McCrary
6,581,162	Method for securely creating, storing and using encryption keys in a computer system.	Angelo, et al.
6,134,661	Computer network security device and method.	Topp
6,578,140	Personal computer having a master computer system and in internet computer system and monitoring a condition of said master and internet computer systems	Policard
PUB Application # 20040054588	E-mail software and method and system for distributing advertisements to client devices that have such e-mail software installed thereon.	Jacobs, Paul E., et al.
PUB Application # 20040034794	System and method for comprehensive general generic protection for computers against malicious programs that may steal information and/or cause damages.	Mayer, Yaron; et al.
PUB Application # 20040006715	System and method for providing security to a remote computer over a network browser interface.	Skrepetos, Nicholas C.
PUB Application # 20030177397	Virus protection in an internet environment.	Samman, Ben
PUB Application # 20030097591	System and method for protecting computer users from web sites hosting computer viruses.	Pham, Khai; et al.
PUB Application # 20030023857	Malware infection suppression.	Hinchliffe, Alexander James; et al.
PUB Application # 20020066016	Access control for computers.	Riordan, James

-continued

U.S. patent or PUB Application Number	Title	Inventor(s)
PUB Application # 20020174349	Detecting malicious alteration of stored computer files.	Wolff, Daniel Joseph; et al.

The above-listed U.S. Patents and U.S. patent applications are incorporated by reference as if reproduced herein in their entirety.

### BACKGROUND

The very popular and ubiquitous rise of the 'personal' computer system as an essential business tool and home appliance, together with the exponential growth of the Internet as a means of providing information flows across a wide variety of connected computing devices, has changed the way people live and work. Information in the form of data files and executable software programs regularly flows across the planetary wide system of interconnected computers and data storage devices.

Popular and ubiquitous computer hardware and software architectures have typically been designed to allow for open interconnection via, for example, the internet, a VPN, a LAN, or a WAN, with information often capable of being freely shared between the interconnected computers. This open interconnection architecture has contributed to the adoption and mainstream usage of these computers and the subsequent interconnection of vast networks of computers. This easy to use system has given rise to the explosive popularity of applications such as email, internet browsing, search engines, interactive gaming, instant messaging, and many, many more.

Although there are definite benefits to this open interconnection architecture, a lack of security against unwanted incursions into the computers main processing and non-volatile memory space has emerged as a significant problem. An aspect of some current computer architectures that has contributed to the security problem is that by default programs are typically allowed to interact with and/or alter other programs and data files, including critical operating system files, such as the windows registry, for example. Current open interconnection architectures have opened the door to a new class of unwanted malicious software generally known as malware. This malware is capable of infiltrating any computer system which is connected to a network of interconnected computer systems. Malware is comprised of, but not limited to, classes of software files known as viruses, worms, Trojan horses, browser hijackers, adware, spyware, pop-up windows, data miners, etc. Such malware attacks are capable of stealing data by sending user keystrokes or information stored on a user's computer back to a host, changing data or destroying data on personal computers and/or servers and/or other computerized devices, especially through the Internet. In the least, these items represent a nuisance that interferes with the smooth operation of the computer system, and in the extreme, can lead to the unauthorized disclosure of confidential information stored on the computer system, significant degradation of computer system performance, or the complete collapse of computer system function.

Malware has recently become much more sophisticated and much more difficult for users to deal with. Once resident on a computer system, many malware programs are designed to protect themselves from deletion. For example, some malware programs comprise a pair of programs running simul-

10 taneously, with each program monitoring the other for deletion. If one of the pair of programs is deleted, the other program installs a replacement within milliseconds. In another example, some malware will run as a Windows program with a .dlls extension, which Windows may not allow a user to delete while it is executing. Malware may also reset a user's browser home page, change browser settings, or hijack search requests and direct such requests to another page or search engine. Further, the malware is often designed to defeat the user's attempts to reset the browser settings to their original values. In another example, some malware programs secretly record user input commands (such as keystrokes), then send the information back to a host computer. This type of malware is capable of stealing important user information, such as passwords, credit account numbers, etc.

15 Many existing computers rely on a special set of instructions which define an operating system (O/S) in order to provide an interface for computer programs and computer components such as the computer's memory and central processing unit (CPU). Many current operating systems have a multi-tasking capability which allows multiple computer programs to run simultaneously, with each program not having to wait for termination of another in order to execute instructions. Multi-tasking O/S's allow programs to execute simultaneously by allowing programs to share resources with other programs. For example, an operating system running multiple programs executing at the same time allows the programs to share the computer's CPU time. Programs which run on the same system, even if not simultaneously with other programs, share space on the same nonvolatile memory storage medium. Programs which are executing simultaneously are presently able to place binaries and data in the same physical memory at the same time, limited to a certain degree by the O/S restrictions and policy, to the extent that these are properly implemented. Memory segments are shared by programs being serviced by the O/S, in the same manner. O/S resources, such as threads, process tables and memory segments, are shared by programs executing simultaneously as well.

20 While allowing programs to share resources has many benefits, there are resulting security related ramifications, particularly regarding malware programs. Security problems include allowing the malware program: to capitalize CPU time, leaving other programs with little or no CPU time; to read, forge, write, delete or otherwise corrupt files created by other programs; to read, forge, write, delete or otherwise corrupt executable files of other programs, including the O/S itself; and to read and write memory locations used by other programs to thus corrupt execution of those programs.

25 In the case of a computer connected to the Internet, the computer may run an O/S, with several user applications, together comprising a known and trusted set of programs, concurrently with an Internet browser, possibly requiring the execution of downloaded code, such as Java applets, or EXE/COM executables, with the latter programs possibly containing malware. Many security features and products are being built by software manufacturers and by O/S programmers to

5

prevent malware infiltrations from taking place, and to ensure the correct level of isolation between programs. Among these are architectural solutions such as rings-of-protection in which different trust levels are assigned to memory portions and tasks, paging which includes mapping of logical memory into physical portions or pages, allowing different tasks to have different mapping, with the pages having different trust levels, and segmentation which involves mapping logical memory into logical portions or segments, each segment having its own trust level wherein each task may reference a different set of segments. Since the sharing capabilities using traditional operating systems are extensive, so are the security features. However, the more complex the security mechanism is, the more options a malware practitioner has to bypass the security and to hack or corrupt other programs or the O/S itself, sometimes using these very features that allow sharing and communication between programs to do so.

Further, regarding malware programs, for virtually every software security mechanism, a malware practitioner has found a way to subvert, or hack around, the security system, allowing a malware program to cause harm to other programs in the shared environment. This includes every operating system and even the Java language, which was designed to create a standard interface, or sandbox, for Internet downloadable programs or applets.

Major vulnerabilities of existing computer systems lies in the architectures of the computer system and of the operating system itself. A typical multi-tasking O/S environment includes an O/S kernel loaded in the computer random access memory (RAM) at start-up of the computer. The O/S kernel is a minimal set of instructions which loads and off-loads resources and resource vectors into RAM as called upon by individual programs executing on the computer. Sometimes, when two or more executing programs require the same resource, such as printer output, for example, the O/S kernel leaves the resource loaded in RAM until all programs have finished with that resource. Other resources, such as disk read and write, are left in RAM while the operating system is running because such resources are more often used than others. The inherent problem with existing architectures is that resources, such as RAM, or a hard disk, are shared by programs simultaneously, giving a malware program a conduit to access and corrupt other programs, or the O/S itself through the shared resource. Furthermore, as many application programs are of a general nature, many features are enabled by default or by the O/S, thus in many cases bypassing the O/S security mechanism. Such is the case when a device driver or daemon is run by the O/S in kernel mode, which enables it unrestricted access to many if not all the resources.

The most common state-of-the-art solutions for preventing malware infiltration are software based, such as blockers, sweepers and firewalls, for example, and hardware based solutions such as router/firewalls. Examples of software designed to counter malware are Norton Systems Works, distributed by the Symantec Corporation, Ad-aware, distributed by the Lavasoft Corporation of Sweeden, Spy Sweeper, distributed by the Webroot Software Corporation, Spyware Guard, distributed by Javacool Software LLC, among others. Currently there are a plethora of freeware, shareware and purchased software programs designed to counter malware by a variety of means. Such anti-malware programs are limited because they can only detect known malware that has already been identified (usually after the malware has already attacked one or more computers).

Network firewalls are typically based on packet filtering, which is limited in principle, since the rules determining

6

which packets to accept and which to reject may contain subjective decisions based on trusting known sites or known applications. However, once security is breached for any reason (for example, due to a software or hardware error, a new piece of malware unrecognized by the anti-malware program or firewall, or an intended deception), a malicious application may take over the computer or server or possibly the entire network and create unlimited damages (directly or indirectly by opening the door to additional malicious applications).

The methods in the prior art are typically comprised of embedded software countermeasures that detect and filter unwanted intrusions in real time, or scan the computer system either at the direction of a user or as a scheduled event. Two problems arise from these methods. In the first instance, a comprehensive scan, detect, and elimination of malware from desired incoming data streams could significantly slow or preclude the interactive nature of many applications such as gaming, messaging, and browsing. In the second instance, newly implemented software screens may be quickly circumvented by malware practitioners who are determined to pass their files through the screen. Newly discovered malware leads to the development of additional screens, which lead to more malware, etc., thus creating an escalating cycle of measure, countermeasure. The basic flaw is that all incoming executable data files must be resident on the computers main processor to perform their desired function. Once resident on that processor, access may be gained to non-volatile memory and other basic computer system elements. Malware exploits this key architectural flaw to infiltrate and compromise computer systems.

The majority of these applications rely upon a scanning engine which searches suspect files for the presence of predetermined malware signatures. These signatures are held in a database which must be constantly updated to reflect the most recently identified malware. Typically, users regularly download replacement databases, either over the Internet, from a received e-mail, or from a CDROM or floppy disc. Users are also expected to update their software engines every so often in order to take advantage of new virus detection techniques (e.g. which may be required when a new strain of malware is detected).

Many of the aforementioned applications are also not effective against security holes, for example, in browsers or e-mail programs, or in the operating system itself. Security holes in critical applications are discovered quite often, and just keeping up with all the patches is cumbersome. Also, without proper generic protection against, for example, Trojan horses, even VPNs (Virtual Private Networks) and other forms of data encryption, including digital signatures, are not totally safe because information can be stolen before or below the encryption layer. Even personal firewalls are typically limited, because once a program is allowed to access the Internet, there are often few limitations on what files may be accessed and transmitted back to a host.

A major problem faced by computer users connected to a network is that the network interface program (a browser, for example) is resident on the same processor as the O/S and other trusted programs, and shares space on a common memory storage medium. Even with security designed into the O/S, malware practitioners have demonstrated great skill in circumventing software security measures to create malware capable of corrupting critical files on the shared memory storage medium. When this happens, users are often faced with a lengthy process of restoring their computer systems to the correct configuration, and often important files are simply lost because no backup exists.

Therefore, what is needed in the art is a means of isolating the network interface program from the main computer system such that the network interface program does not share a common memory storage area with other trusted programs. The network interface program may be advantageously given access to a separate, protected memory area, while being unable to initiate access to the main computer's memory storage area. With the network interface program constrained in this way, malware programs are rendered unable to automatically corrupt critical system and user files located on the main memory storage area. If a malware infection occurs, a user would be able to completely clean the malware infection from the computer using a variety of methods. A user could simply delete all files contained in the protected memory area, and restore them from an image residing on the main memory area, for example.

Other discussions of malware, its effects on computer systems, techniques used by malware practitioners to install malware, and techniques for detection and removal, may be found in the published literature, and in some of the patents and applications previously incorporated by reference. Reference to malware may be found in a technical white paper entitled "Spyware, Adware, and Peer-to-Peer Networks: The Hidden Threat to Corporate Security.", by Kevin Townsend, © Pest Patrol Inc. 2003. Pest Patrol is a Carlisle, Pa. based developer of software security tools. Another reference is a technical white paper entitled "Beyond Viruses: Why anti-virus software is no longer enough." by David Stang, PhD, © Pest Patrol Inc. 2002. Yet another reference is "The Web: Threat or Menace?" from "Firewalls and Internet Security: Repelling the Wily Hacker", Second Edition, Addison-Wesley, ISBN 0-201-63466-X, Copyright 2003. The foregoing references are incorporated by reference as if reproduced herein in their entirety.

#### SUMMARY OF THE INVENTION

Embodiments of the present invention achieve technical advantages as a system and method for protecting a computer system from malicious software attacks via a network connection.

It is an object of the present invention to provide a computer system capable of preventing malware programs from automatically corrupting critical user and system files.

It is another object of the present invention to confine any malware infection that may occur to a separate, protected part of the computer system.

It is another object of the present invention to provide a user with an easy and comprehensive method of removing the malware infection, even if the user's anti-malware software is incapable of detecting and/or removing the malware infection.

It is another object of the present invention to provide a user with an easy and comprehensive method of restoring critical system and user files that may have been corrupted by a malware infection.

It is another object of the present invention to provide a computer system configured such that attempts by malware to record and report data entry by the computer user via input devices such as keyboards, mouse clicks, microphones, or any other data input devices are effectively blocked.

It is another object of the present invention to provide a computer system capable of executing instructions in a first logical process, wherein the first logical process is capable of accessing data contained in a first memory space and a second memory space.

It is another object of the present invention to provide a computer system capable of executing instructions in a second logical process, wherein the second logical process is capable of accessing data contained in the second memory space, the second logical process being further capable of exchanging data across a network of one or more computers.

It is another object of the present invention to provide a computer system capable of displaying, in a windowed format on a display terminal, data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to the display terminal.

It is another object of the present invention to provide a computer system configured such that a malware program downloaded from the network and executing as part of the second logical process is incapable of initiating access to the first memory space.

It is another object of the present invention to provide a computer system configured such that corrupted data files residing on the second memory space may be restored from an image residing on the first memory space.

It is another object of the present invention to provide a computer system configured such that data files residing on the second memory space may be automatically deleted when the second logical process is terminated.

It is another object of the present invention to provide a computer system configured such that the second electronic data processor and the video processor are co-located on a circuit card, the circuit card being communicatively coupled to the first electronic data processor.

These objects and other advantages are provided by a preferred embodiment of the present invention wherein a computer system comprising a first electronic data processor is communicatively coupled to a first memory space and to a second memory space, a second electronic data processor is communicatively coupled to the second memory space and to a network interface device, wherein the second electronic data processor is capable of exchanging data across a network of one or more computers via the network interface device, a video processor is adapted to combine video data from the first and second electronic data processors and transmit the combined video data to a display terminal for displaying the combined video data in a windowed format, wherein the computer system is configured such that a malware program downloaded from the network and executing on the second electronic data processor is incapable of initiating access to the first memory space.

#### BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, and the advantages thereof, reference is now made to the following descriptions taken in conjunction with the accompanying drawings, in which:

FIG. 1 illustrates a preferred embodiment of an exemplary computer system according to the principles of the present invention;

FIG. 2 illustrates a preferred embodiment of an exemplary protected process flow according to the principles of the present invention;

FIG. 3 illustrates a preferred embodiment of an exemplary file download process according to the principles of the present invention;

FIG. 4 illustrates a preferred embodiment of an exemplary memory restoration process according to the principles of the present invention;

FIG. 5 illustrates a preferred embodiment of an exemplary automatic memory restoration and cleaning process according to the principles of the present invention;

FIG. 6 illustrates a preferred embodiment of an exemplary interactive network process flow according to the principles of the present invention;

FIG. 7 illustrates a preferred embodiment of an exemplary computer system according to the principles of the present invention;

FIG. 8 illustrates a preferred embodiment of an exemplary computer system according to the principles of the present invention;

FIG. 9 illustrates a preferred embodiment of an exemplary computer system according to the principles of the present invention;

FIG. 10 illustrates a preferred embodiment of an exemplary protected process flow according to the principles of the present invention.

#### DETAILED DESCRIPTION OF THE ILLUSTRATED EMBODIMENTS

The making and using of the presently preferred embodiments are discussed in detail below. It should be appreciated, however, that the present invention provides many applicable inventive concepts that can be embodied in a wide variety of specific contexts. The specific embodiments discussed are merely illustrative of specific ways to make and use the invention, and do not limit the scope of the invention.

A computer system, constructed in accordance with a preferred embodiment of the present invention, is illustrated in FIG. 1. Computer system 100 may represent, for example, a personal computer (PC) system, a server, a portable computer, such as a notebook computer, or any data processing system, a personal digital assistant (PDA), a communication device such as a cell phone, or device that is capable of being connected to a network of one or more computers. System 100 comprises a first processor 120 (P1) communicatively coupled to a first memory and data storage area 110 (M1). P1 100 may comprise, for example, a microprocessor, such as a Pentium® 4 processor, manufactured by the Intel Corporation, or a Power PC® processor, manufactured by the IBM Corporation. Other electronic data processors manufactured by other companies, including but not limited to electronic data processors realized in Application Specific Integrated Circuits (ASICs) or in Field Programmable Gate Arrays (FPGAs), are within the spirit and scope of the present invention.

The first memory and data storage area 110 may comprise both volatile and nonvolatile memory devices, such as DRAMs and hard drives, respectively. Any memory structure and/or device capable of being communicatively coupled to P1 may be advantageously used in the present invention. M1 may be used to store, for example, critical operating system files, user data and applications, interim results of calculations, etc. The many uses of computer memory are well understood by those skilled in the art, and will not be discussed further here. One may refer to several of the aforementioned patents and applications incorporated by reference, in addition to other references, for a discussion of existing computer architectures and uses of computer memory. Also part of system 100 is user interface 150, which may comprise, for example, a keyboard, mouse or other pointing device, microphone, pen pad, etc. Any device or method capable of inputting commands and/or data from a user 160 to computer system 100 may be used to advantage. A video processor 170 is used to format information for display and transmit the display information to a video dis-

play device 180, which is viewed by user 160. Video processor 170 typically includes an associated video memory area, which may be dedicated to the video processor, or shared with other resources. It is understood in the art that the video processor 170 may be part of processor P1 120, in that it may be integrated onto the microprocessor chip. Video processor 170 may also comprise a processor IC located on a video graphics card, which is communicatively coupled to a computer motherboard. Additionally, video processor 170 may comprise circuitry located on the computer motherboard. Further still, functions of video processor 170 may be split between the processor, motherboard, or separate video graphics card.

It is often desirable to connect computer system 100 to a network of one or more computer devices 195, such as the Internet, a LAN, WAN, VPN, etc. This connection may be accomplished via network interface device 190, which may comprise, for example, a telephone modem, a cable modem, a DSL line, a router, gateway, hub, etc. Any device capable of interfacing with the network 195 may be used, via a wired connection, a wireless connection, or an optical connection, for example. Network interface device 190 may connect to network 195 through one or more additional network interface devices (not shown). For example, network interface device 190 may comprise a gateway or router, connected to a cable modem, with the cable modem connected to network 195. Of course, other configurations are within the spirit and scope of the present teachings.

In accordance with a preferred embodiment of the present invention, network 195 is isolated from the first processor 120 and memory 110 by a second processor 140 (P2). Second processor 140 may comprise any electronic data processor, such as the devices previously described as applicable to first processor 120. Communicatively coupled to P2 140 is second memory and data storage area 130 (M2), which may comprise any memory device or devices, such as the devices previously described as applicable to first memory 110.

The architecture of computer system 100 is designed to be capable of protecting memory 110 from malware initiated intrusions, and preventing malware from initiating unwanted processes on first processor 120. This is accomplished by using second processor 140 to isolate 110 and 120 from network 195. In a preferred embodiment, P2 140 is communicatively coupled to memory storage area M2 130, and may be configured such that P2 140 is incapable of initiating access to memory storage area M1 110. For example, P2 140 may be capable of accessing memory storage area M1 110 with the strict permission of user 160, either through a real time interaction or via stored configuration or commands. Such a configuration may be desirable in a multi-core or multi processor system, where user 160 may wish to use P2 140 in either a protected mode or an unprotected mode, depending on the application. However, user 160 is capable of denying P2 140 the capability of initiating access to memory storage area M1 110 without the user's permission. P1 120 is communicatively coupled to both memory areas M1 110 and M2 130, thereby enabling P1 120 to access data downloaded from the network 195. In the presently described embodiment, any malware that has intruded the 130-140 system is thus confined to the 130-140 system, and may be configured to be incapable of automatically corrupting data contained on M1 110, or of automatically initiating an unwanted process on P1 120.

This and other features of the present teachings may be illustrated with reference to the example process flow 200 of FIG. 2. Computer user 160 wishes to connect to network 195 via for example, a browser program such as Internet Explorer

## 11

or Netscape Navigator. Of course, other methods of connecting to network 195 may be used. User 160 inputs commands to open a protected process (e.g. a browser program in this example) at step 210. At step 220, 1<sup>st</sup> processor 120 instructs 2<sup>nd</sup> processor 140 to initiate the protected process and open one or more process windows. Second processor 140, in conjunction with memory 130, then interacts with the network 195 via network interface device 190, receiving and transmitting the data necessary to execute the desired protected process, such as browsing the internet or communication via e-mail. Second processor 140 and memory 130 act as a separate computer system, interacting with network 195 while isolating network 195 from the first processor 120 and memory 110. Memory 130 may store critical application and system files required by second processor 140 to execute the desired tasks. Memory 130 also stores data necessary to carry out the desired protected process. In the example of FIG. 2, first processor 120 receives user interface data from user 160, and passes user interface data to second processor 140 when the protected process window is selected or active, illustrated at step 230. User interface data, such as keystrokes for example, may be advantageously encrypted by P1 120 before passing the data to P2 140, with network interface device 190 possibly decrypting the data prior to transmitting the data to network 195. Encrypting, for example keystroke data, may disrupt the efforts of spyware programs designed to store user keystrokes for later transmission to a host computer. Second processor 140 generates video data for the protected process window(s) and passes the video data to video processor 170, for eventual display on video display 180, shown at step 240. Video processor 170 then interleaves the video data from all processes being executed by first processor 120 and second processor 140, at step 250. While there are many applicable methods for displaying video data from multiple sources, one such method was described in U.S. Pat. No. 5,751,979, entitled "Video hardware for protected, multiprocessing systems", previously incorporated by reference.

In accordance with a preferred embodiment of the present invention, if any malware is downloaded from network 195, it is stored in memory 130, and/or run as a process on second processor 140. In the configuration of computer system 100, any downloaded malware is rendered incapable of self initiating access to memory 110 or first processor 120, because second processor 140 is rendered incapable of initiating access to 110 and 120 without a direct or stored command from user 160. Any malware infection is thus confined. If a malware attack corrupts files and/or disrupts the operation of the 130-140 system, the user may easily shut down the corrupted process and restore the corrupted files from a protected image stored on memory 110, for example.

In accordance with a preferred embodiment of the present invention, the operating system controlling the 110-120 system may be different from an operating system controlling the protected 130-140 system. Conversely, a common operating system may control both the 110-120 system and the protected 130-140 system.

A user 160 may find it desirable to transfer files from the protected 130-140 system to the 110-120 system. User 160 may find it necessary, for example, to transfer an attachment from an e-mail message stored on memory 130 to the 110-120 system for further processing, modification, etc. In this case, the computer system 100 may go through a process whereby a file or other data is transferred from the 130-140 system to the 110-120 system, exemplified by the process 300 illustrated in FIG. 3.

In accordance with a preferred embodiment of the present invention, at step 310, user 160 selects one or more data files

## 12

to download from network 195. The desired data is downloaded to the 130-140 system at step 320. The user 160 then directs computer system 100 to move the desired file(s) from the 130-140 system to the 110-120 system at step 330. P1 120 may then perform a malware scan on the desired files, either in real time as the data is being transferred, or while the data still resides in M2 130 (step 340). Alternatively, P2 140 may perform the malware scan. At step 350, processor P2 140 (or P1 120) determines if malware has been detected in the desired file(s), and thus P1 120 makes a decision. If no malware is detected, the file(s) are moved or copied onto M2 110 at step 360. If malware is detected, the data file(s) are quarantined on M2 130, and the data file(s), if transferred to M1 100, are erased or quarantined. Once malware is detected, the user 160 may be alerted of the detection (step 370). Either as a result of user input or stored configuration commands, the infected file(s) are deleted, cleaned, or quarantined on M2 130, at step 380.

The user 160 would of course understand the dangers inherent in transferring downloaded files from the 130-140 system to the 110-120 system. For example, the user's anti-malware software may not be up to date, or may simply be unable to detect certain types of malware. Also, the malware itself may be so new that the user's anti-malware definitions have not been updated as yet. Therefore the user may wish to keep the files on the 130-140 system for some period of time. Consequently, it may be desirable to have resident on the 130-140 system a variety of application software such as readers, thereby allowing the user to examine the files without risking transferring the files to the 110-120 system. These reader programs, such as Adobe Acrobat Reader, by the Adobe Systems Corporation, or Visio reader, by the Microsoft Corporation, are typically subset application programs of the full featured application programs, and may thus require far less memory space than the full application. Additionally, software companies often distribute the reader programs for free (or a nominal fee), thereby providing advertising for the full featured application in the hopes that it will be eventually purchased by the user. This reader application may be opened and executed on the 130-140 system in a manner similar to the process described in FIG. 2. Of course, a user 160 may also load a full application into the 130-140 system, enabling processing and modification of a downloaded file fully in the protected space, without risking a transfer of the file to the 110-120 system.

In the event the 130-140 system becomes infected with malware, the user 160 may wish to clean the 130-140 system. This cleaning may be accomplished by running an anti-malware application on the 130-140 system. However, if the infection is too severe for the anti-malware software to clean, or if the malware is undetectable by the user's anti-malware software, the user may wish to restore critical system files (or other user data files) for the 130-140 system from a protected image stored on M1 100, for example. It is of course understood that the critical system file image may be restored from another device, such as a removable drive or a CD, for example. The user may however consider it more convenient to restore the critical system files from an image on M1 100.

In accordance with a preferred embodiment of the present invention, an exemplary process for restoring M2 130 from M1 110 is illustrated by process 400 in FIG. 4. At step 410, malware is detected or suspected to be infecting the 130-140 system. The user instructs P1 120 to reload critical system files onto M2 130 from a protected image on M1 110, at step 420. Depending on the severity of the infection, P1 120 may scan all or part of the data contained on M2 130 for malware, and may scan all processes currently running on P2 140. The

13

scan may be initiated by direct instructions from the user, or by stored configuration commands, for example (step 430). P1 120 may delete all or part of the data contained on M2. P1 120 may also reset P2 140 and/or delete the contents of any RAM communicatively coupled to P2 140 (step 440). Once the 130-140 system has been adequately cleaned, clean critical system files are loaded onto M2 130 from any of the sources previously mentioned, preferably an image stored on M1 110 (step 450). The 130-140 may now be rebooted and/or reinitialized from the clean critical system files. In an extreme case where the malware resists deletion by the operating system, the user may elect to do a low level format on the M1 110 memory in order to ensure that the malware infection has been cleaned.

In accordance with a preferred embodiment of the present invention, a user 160 may consider it advantageous for the 130-140 system to be automatically reinitialized from clean critical system files when a protected process window is opened. In this way, the new protected process is much less likely to be affected by an infection from a previous protected process session. Of course, a user may have a plurality of protected processes open and running during a protected process session. It may only be necessary to automatically reinitialize from clean critical system files when the first protected process is opened during a session. Subsequent protected processes may not require automatic re-initialization from clean critical system files. An exemplary automatic re-initialization from clean critical system files is illustrated by steps 510, 520 and 530 in FIG. 5a. Additionally, processes running on P2 140 may be automatically scanned and compared with an allowed process list, particularly as a protected process is started up. If any process is detected which is not on the allowed list, the user may be alerted that a possible malware infection has occurred. A user may then choose to scan or clean the system, or inspect the unknown process to determine if the process will be allowed to continue to execute. A user may also update the list of allowed processes from time to time as new, legitimate processes are added, for example, by a browser software update.

In accordance with a preferred embodiment of the present invention, a user 160 may consider it advantageous for the 130-140 system to be automatically cleaned when a protected process window is closed. In this way, any detected or undetected malware infections are much less likely to affect a future protected process session. It may only be necessary to automatically clean the 130-140 system when the last protected process is closed during a session. An exemplary automatic cleaning process is illustrated by steps 540, 550, 560, 570 and 580 in FIG. 5b. The memory M2 130 and processor P2 140 may be automatically scanned for malware infections as the protected process session closes. Infected files may be deleted or quarantined automatically. Additionally, there may be a variety of files that a user may wish to have automatically cleaned or deleted upon closing a protected process session. For example, temporary internet files, cookies, browser plug-ins, etc., may be deleted or scanned for malware automatically. A user may also wish to have websites that contributed to a malware infection noted, and may wish to place the offending websites in a block list, such that the offending websites cannot be accessed in the future without the user specifically authorizing access. As part of the malware scan, the malware scanner may automatically log the offending website(s), and block future access. Also, the P2 140 processor and any associated non-volatile memory may be reset and/or erased as the protected process session is closed. The exemplary automatic cleaning process illustrated in FIG. 5b

14

may therefore reduce the risk of a malware infection being carried over to a future protected process session.

Interactive network processes such as interactive gaming have become very popular in recent years. In current interactive gaming processes, a user may log onto a game host located on network 195, or connect to other computers whose users wish to participate in the game. Computer games, such as Quake 3. Arena, by Id Software Incorporated, or Call of Duty, by Activision Incorporated, are just two examples of the plethora of games available that may be played interactively over a network. The user's computer system typically provides the bulk of the processing power and video graphics generation required to display the often fast moving and richly detailed three dimensional game environments. Information about the current and new state of the game is exchanged between various users' computer systems, often in real time. With this type of process, a relatively modest amount of data is required to be exchanged between users, or a user and the host, with the bulk of the processing, data manipulation, and graphics generation being handled by the user's local machine. However, this open network connection may become a conduit for malware practitioners to exploit, allowing malware to be downloaded onto a user's computer during a gaming session, often without the user being aware of the malware transfer. It would be advantageous, therefore, for a computer system to be much less susceptible to malware attacks during gaming sessions.

In accordance with a preferred embodiment of the present invention, an exemplary process flow 600, illustrated in FIG. 6, allows an interactive network process, such as online gaming, to be carried out on computer system 100. A user initiates an interactive network process via 2<sup>nd</sup> processor P2 140 (step 610). P2 140 receives interactive network process status data from network connection (step 620). P2 140 informs 1st processor P1 120 that interactive network process status data is available (step 630). P1 120 retrieves interactive network process status data from P2 140 and uses the status data to update the interactive network process and update video display (step 640). P1 120 then passes the updated interactive network process status data to P2 140 (step 650). P2 140 then sends the updated interactive network process status data to the network via network connection 195 (step 660). The exemplary process 600, or a process functionally equivalent, is carried out continuously as long as the interactive process is running.

By using exemplary process 600 (or an equivalent), computer system 100 is capable of actively deciding what data to download and use, and what data to discard or scan for malware. The game status data is buffered prior to loading it onto the 110-120 system. The 110-120 system may be advantageously configured to only accept game status information in the proper format, thereby minimizing the chance that a malware practitioner could deceptively load malware onto the 110-120 system.

Additionally, computer system 100 could be configured such that system 130-140 is powerful enough to process the interactive network process without exchanging information with the 110-120 system. Such a configuration may be more secure, as a conduit between the 110-120 system and the 130-140 system may not be necessarily opened. The 130-140 system may contain all the necessary files to facilitate the interactive network process. Higher end computers, workstations, and servers often contain dual (or more) processors, such as the Mac G5, manufactured by the Apple Computer Corporation, or a single physical processor with a multiple processor core. Often, the processors in these multi-processor machines are of equal or comparable processing power. In



15

such a configuration, one processor may be dedicated to performing functions equivalent to those described for P1 120, with a second processor performing the functions equivalent to those described for P2 140. A computer system 100 employing multiple processors may be advantageously configured such that one of the processors is dedicated to protected processes only when a network process is active. When a user is not accessing a network, the multiple processors in a computer system may be dedicated to other processes, such as performing complex calculations or simulations, or running complex non-network interactive gaming processes, for example. Alternatively, the computer system 100 may be configured such that the 110-120 system simply transfers required files to the video processor 170 or the 130-140 system at the appropriate time to facilitate the interactive network process. The 110-120 system could be commanded to retrieve and transfer the files at the command of the video processor, or at the command of the 130-140 system, or a combination of both.

In accordance with embodiments of the present invention, computer system 100 may be configured in a variety of ways, while still remaining within the spirit and scope of the present teachings. One such exemplary embodiment is illustrated in FIG. 7. Subsystem 700 of computer system 100 comprises a video processor 770, a second processor 740, and a second memory data storage area 730. The demarcation line illustrated by subsystem 700 may be either physical or logical. For example, subsystem 700 may comprise an add-on card, such as a high end video card, or a video/network card. If configured in this exemplary manner, a user could upgrade an existing computer system to take advantage of the teachings of the present invention. Subsystem 700 may be plugged into the main motherboard of an existing computer, for example. The motherboard connector may be already communicatively coupled to the 110-120 system, thereby facilitating the system upgrade. The network interface device 190 may be connected directly to subsystem 700, or network interface device 190 could be integrated as part of subsystem 700. Memory data storage area 730 may comprise any of the volatile and/or non-volatile memory types previously described, or any combination thereof, or any suitable memory storage medium, for example. Alternatively, subsystem 700 may be located on the motherboard, as opposed to an add-on card. Further still, portions of subsystem 700, such as video processor 770, and/or second processor 740, for example, may be integrated together with P1 120. It is understood that functions described herein may be configured in a wide variety of ways, without departing from the spirit and scope of the present teachings.

In accordance with a preferred embodiment of the present invention, an alternate configuration for computer system 100 is illustrated in FIG. 8. Subsystem 800 of computer system 100 comprises a video processor 870, a second processor 840, and a second memory data storage area 830. The demarcation line illustrated by subsystem 800 may be either physical or logical. For example, subsystem 800 may comprise an add-on card, such as a high end video card, or a video/network card. If configured in this exemplary manner, a user could upgrade an existing computer system to take advantage of features of the present invention. In the exemplary embodiment of FIG. 8, second processor 840 and video processor 870 are integrated together, perhaps on a common integrated circuit. Such a configuration may help to reduce the cost of subsystem 800, and/or improve the performance. Additionally, a circuit designer may find it advantageous to integrate 840 and 870 together to facilitate communication between the functions. It

16

is understood that such an integration of functions may create a device in which an external user may find it difficult to distinguish where the function of 870 ends and the function of 840 begins, and vice versa. Such a device, however, would remain within the spirit and scope of the present teachings.

In accordance with a preferred embodiment of the present invention, an alternate configuration for computer system 100 is illustrated in FIG. 9. Computer system 100 comprises a video processor 970, processor 960, and a memory data storage area 950. Processor 960 may further comprise multiple processor cores, illustrated by 1<sup>st</sup> processor 920 and 2<sup>nd</sup> processor 940. It is understood that processor 960 may contain more than 2 processor cores. Microprocessors manufactured with multiple processor cores are becoming common in the industry, and such multi-core processors may be particularly advantageous when used in accordance with the present teachings. Memory data storage area 950 may further comprise 1<sup>st</sup> memory data storage area 910 and 2<sup>nd</sup> memory data storage area 930. Memory areas 910 and 930 may comprise, for example, different partitions on a single hard drive, and/or different address ranges in a RAM bank.

Referring again to FIG. 9, the functions carried out by processors 920 and 940 may comprise separate, secure logical processes executing on the same physical processor. For example, a first logical process may comprise executing instructions necessary to carry out the functions of an operating system, or the first logical process may comprise executing instructions necessary to carry out the functions of a first computer program, including but not limited to a word processor. A second logical process may comprise executing instructions necessary to carry out the functions of a web browser program, or may comprise executing instructions necessary to carry out the functions of an instant messenger program, for example. A computer system 100 constructed in accordance with the principles of the present invention would be capable of disallowing a secure logical process, such as the second logical process described above, access to certain memory spaces, and/or disallowing a secure logical process from initiating access to another logical process. For example, the functions carried out by P2 140 (FIG. 1) may comprise a secure logical process, which may be configured to be unable to automatically initiate access to either M1 110 or another logical process performing the functions of P1 120. Additionally, memory areas 910 and 930 may comprise separate, isolated memory zones within a common physical memory space, such as separate partitions within the same hard drive, for example.

Some malware programs are designed to secretly record user input commands (such as keystrokes, for example), then send the information back to a host computer. This type of malware is capable of stealing important user information, such as passwords, bank account numbers, social security numbers, driver's license numbers, credit account numbers, etc. Theft of such personal information could result in the theft of actual assets (money or securities, etc.) or perhaps used for identity theft, among other malicious intents. Clearly, a computer system capable of ensuring the protection of such sensitive information would be desirable.

In accordance with an embodiment of the present invention, a computer system is configured such that attempts by malware to record and report data entry by the computer user via input devices such as keyboards, mouse clicks, microphones, or any other data input devices are effectively blocked. Encryption of user input data, such as keystrokes, is an effective means of protecting such data from theft by malware. Specific techniques used for data encryption and decryption are well known in the art, and need not be dis-

cussed further here. There are many examples in the art that may be examined to better understand various encryption/decryption techniques and the use of encryption/decryption in computer systems. Among these are U.S. Pat. No. 6,581,162 entitled "Method for securely creating, storing and using encryption keys in a computer system." issued to Angelo, et al., and U.S. Pat. No. 6,134,661 entitled "Computer network security device and method." Issued to Topp. The aforementioned patents have been previously incorporated by reference.

In accordance with the present teachings, a method of operating a computer system involving data encryption is described. In step 1010, a user opens a protected process where some level of data encryption is desired, for example, the encryption of sensitive user interface data or user files. Other data may be encrypted as desired. At step 1020, processor P1 120 instructs processor P2 140 to initiate a protected process and open a process window. P1 120 encrypts the sensitive data and passes the user interface data to P2 140 when a P2 140 window is selected or active (step 1030). P2 140 generates video data for the P2 140 process window(s) and passes the video data to video processor 170 (step 1040). Video processor 170 decrypts the sensitive data and interleaves the video data from all P1 and P2 processes (step 1050). P2 140 passes the encrypted sensitive data to network interface device 190 (step 1060). Network interface device 190 decrypts the sensitive data and passes the decrypted sensitive data to network 195. Of course, other methods of operating a computer system in which data is encrypted prior to being passed to P2 140, and decrypted after leaving the control of P2 140, are within the spirit and scope of the present teachings.

In accordance with a preferred embodiment of the present invention, data desired to be protected is encrypted prior to sending the data to processor P2 140, which may be running one or more malware processes. Processor P2 140 does not have visibility to the decryption keys, and is therefore unable to decrypt the data. Data may be decrypted by network interface device 190 prior to forwarding the data on to network 195. Conversely, encrypted data may be sent directly over the network for decryption by another computer system, including, for example, an internet banking host computer. Decryption keys may be passed between P1 120 and network interface device 190 via a communication link 191. Video processor 170 may decrypt the data prior to displaying the data on video display 180, with decryption keys possibly passed between P1 120 and video processor 170 via a communication link 171. Conversely, data may be passed directly to video processor 170 via a communication link 151.

A user 160 may wish to encrypt just a portion of the data destined for the network, such as passwords, credit card numbers, etc. Conversely, a user may wish to encrypt large blocks of data, such as e-mails or large application files containing sensitive text and/or graphics. Instructions may be passed to network interface device 190 directing 190 to decrypt one or more specific data blocks prior to sending the data blocks to network 195. Conversely, instructions may be passed to network interface device 190 directing 190 to pass one or more specific data blocks to network 195 without decryption.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications and combinations of the illustrative embodiments, as well as other embodiments of the invention, will be apparent to persons skilled in the art upon reference to the description. It is therefore intended that the appended claims encompass any such modifications or embodiments.

What is claimed is:

1. A method of operating a computer system having at least a first and second electronic data processor capable of executing instructions using a common operating system, comprising the steps of:
  - 5 executing instructions in a first logical process within the common operating system using the first electronic data processor, wherein the first logical process is capable of accessing data contained in a first memory space and a second memory space;
  - 10 executing instructions in a second logical process within the common operating system using the second electronic data processor, wherein the second logical process is capable of accessing data contained in the second memory space, the second logical process being further capable of exchanging data across a network of one or more computers;
  - 15 displaying, in a windowed format on a display terminal, data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to the display terminal;
  - 20 wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second logical process.
  - 25 2. The method of claim 1 wherein the first memory space and the second memory space comprise separate regions of a common memory space.
  - 30 3. The method of claim 1 wherein the second logical process is selected from the group consisting of; an electronic mail process, an instant messaging process, an internet browser process, an interactive gaming process, a virtual private network (VPN) process, and a reader application process.
  - 35 4. The method of claim 1 wherein the first logical process receives user interface data, and passes the user interface data to the second logical process.
  - 40 5. The method of claim 1 wherein the first and second electronic data processors are part of a multi-core electronic data processor.
  - 45 6. The method of claim 1 and further comprising the step of restoring at least one corrupted data file residing on the second memory space from an image residing on the first memory space.
  - 50 7. The method of claim 1 and further comprising the step of automatically deleting at least one data file residing on the second memory space when the second logical process is terminated.
  - 55 8. The method of claim 1 and further comprising the steps of:
    - encrypting data with the first logical process;
    - transferring the encrypted data from the first logical process to the second logical process;
    - transferring the encrypted data from the second logical process to the network interface device.
  - 60 9. The method of claim 8 and further comprising the steps of:
    - 65 decrypting the data with the network interface device;
    - transferring the decrypted data from the network interface device to the network.
  10. A multi-processor computer system using a common operating system, comprising:

19

a first electronic data processor capable of executing instructions using the common operating system and communicatively coupled to a first memory space and a second memory space;

a second electronic data processor capable of executing instructions using the common operating system and communicatively coupled to the second memory space and to a network interface device, wherein the second electronic data processor is capable of exchanging data across a network of one or more computers via the network interface device;

a video processor adapted to combine video data from the first and second electronic data processors and transmit the combined video data to a display terminal for displaying the combined video data in a windowed format; wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing on the second electronic data processor.

**11.** The computer system of claim **10** wherein the first memory space and the second memory space comprise separate regions of a common memory space.

**12.** The computer system of claim **10** wherein the first and second electronic data processors are part of a dual processor computer system.

**13.** The computer system of claim **10** wherein the second electronic data processor and the video processor are co-located on a circuit card, the circuit card being communicatively coupled to the first electronic data processor.

**14.** The computer system of claim **10** wherein the computer system is configured such that the first electronic data processor is protected from executing instructions initiated by a malware process downloaded from the network and executing on the second electronic data processor.

**15.** A multi-processor computer system using a common operating system, comprising:

at least a first and second electronic data processor capable of executing instructions using the common operating system;

at least a first and second memory space;

a video processor;

wherein the first and second electronic data processors, first and second memory space, and video processor are configured for performing the steps of:

20

executing instructions in a first logical process with the first electronic data processor, wherein the first logical process is executing within the common operating system and is capable of accessing data contained in the first memory space and the second memory space;

executing instructions in a second logical process with the second electronic data processor, wherein the second logical process is executing within the common operating system and is capable of accessing data contained in the second memory space, the second logical process being further capable of exchanging data across a network of one or more computers;

displaying, in a windowed format on a display terminal, data from the first logical process and the second logical process, wherein the video processor is adapted to combine data from the first and second logical processes and transmit the combined data to the display terminal;

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second logical process.

**16.** The computer system of claim **15** wherein the computer system is further configured such that the first logical process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second logical process.

**17.** The computer system of claim **15** and further comprising: at least one network interface device capable of exchanging data with both the second logical process and with the network.

**18.** The computer system of claim **17** wherein the network interface device is capable of decrypting data received from the second logical process and transmitting the decrypted data to the network while preventing the second logical process from accessing the decrypted data.

**19.** The computer system of claim **15** wherein the at least one electronic data processor is selected from the group consisting of: a multi-core electronic data processor; dual electronic data processors; and multiple electronic data processors.

**20.** The computer system of claim **15** and further configured for performing the step of: restoring at least one corrupted data file residing on the second memory space from an image residing on the first memory space.

\* \* \* \* \*

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**REISSUE APPLICATION DECLARATION BY THE INVENTOR**

Docket Number (Optional)

ARAC-01RE1

I hereby declare that:

Each inventor's residence, mailing address and citizenship are stated below next to their name.

I believe the inventors named below to be the original and first inventor(s) of the subject matter which is described and claimed in patent number 7,484,247, granted Jan 27, 2009 and for which a reissue patent is sought on the invention entitled System and method for protecting a computer system from malicious software,

the specification of which

is attached hereto.

was filed on \_\_\_\_\_ as reissue application number \_\_\_\_\_

and was amended on \_\_\_\_\_ .  
(If applicable)

I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b). Attached is form PTO/SB/02B (or equivalent) listing the foreign applications.

I verily believe the original patent to be wholly or partly inoperative or invalid, for the reasons described below. (Check all boxes that apply.)

by reason of a defective specification or drawing.

by reason of the patentee claiming more or less than he had the right to claim in the patent.

by reason of other errors.

At least one error upon which reissue is based is described below. If the reissue is a broadening reissue, such must be stated with an explanation as to the nature of the broadening:

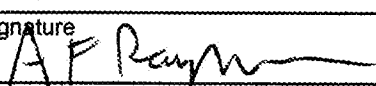
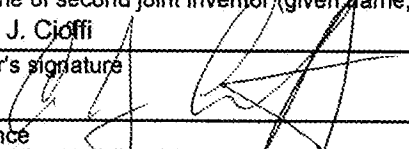
The patentees have claimed less than they had the right to claim and have filed a broadening reissue. At least one error is the failure to claim subject matter disclosed in the specification pertaining to a portable computer wherein attempts by malware to record data entry by the computer user are effectively blocked.

[Page 1 of 2]

This collection of information is required by 37 CFR 1.175. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

(REISSUE APPLICATION DECLARATION BY THE INVENTOR, page 2)		Docket Number (Optional) ARAC-01RE1			
All errors corrected in this reissue application arose without any deceptive intention on the part of the applicant.					
Note: To appoint a power of attorney, use form PTO/SB/81.					
Correspondence Address: Direct all communications about the application to:					
<input type="checkbox"/> The address associated with Customer Number: <input type="text"/>					
<b>OR</b>					
<input checked="" type="checkbox"/> Firm or Individual Name	Allen f. Rozman				
Address	6402 Wildlife Trail				
City	Garland	State	Texas	Zip	75044
Country	USA				
Telephone	214-478-2172	Email	arozman@verizon.net		
<b>WARNING:</b>					
Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.					
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine and imprisonment, or both, under 18 U.S.C. 1001, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this declaration is directed.					
Full name of sole or first inventor (given name, family name) Allen F. Rozman					
Inventor's signature 			Date 3-9-10		
Residence 6402 Wildlife Trail Garland, Texas 75044			Citizenship USA		
Mailing Address 6402 Wildlife Trail Garland, Texas 75044					
Full name of second joint inventor (given name, family name) Alfonso J. Cioffi					
Inventor's signature 			Date 3-9-10		
Residence 719 Mockingbird Dr, Murphy, Texas 75094			Citizenship USA		
Mailing Address 719 Mockingbird Dr, Murphy, Texas 75094					
<input type="checkbox"/> Additional joint inventors or legal representative(s) are named on separately numbered sheets forms PTO/SB/02A or 02LR attached hereto.					

## Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number <b>12/720,147</b>	Filing Date <b>03/09/2010</b>	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)
<input checked="" type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A	<b>165</b>	N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A		N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	20 minus 20 =	* 0	X \$26 =	<b>0</b>	OR	X \$ =
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	3 minus 3 =	* 0	X \$110 =	<b>0</b>	OR	X \$ =
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>						
			TOTAL	<b>165</b>	TOTAL	

\* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT	<b>03/09/2010</b>	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 57	Minus ** 20	= 37	X \$26 =	<b>962</b>	OR	X \$ =
	Independent (37 CFR 1.16(h))	* 6	Minus *** 3	= 3	X \$110 =	<b>330</b>	OR	X \$ =
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR	
					TOTAL ADD'L FEE	<b>1292</b>	OR	TOTAL ADD'L FEE

	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	X \$ =		OR	X \$ =
	Independent (37 CFR 1.16(h))	*	Minus ***	=	X \$ =		OR	X \$ =
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:  
 /JESSICA GAYNOR/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number <b>12/720,147</b>	Filing Date <b>03/09/2010</b>	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)
<input checked="" type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A	<b>165</b>	N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A		N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	20 minus 20 =	* 0	X \$26 =	<b>0</b>	OR	X \$ =
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	3 minus 3 =	* 0	X \$110 =	<b>0</b>	OR	X \$ =
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>						
			TOTAL	<b>165</b>	TOTAL	

\* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR		
AMENDMENT	03/09/2010	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 57	Minus ** 20	= 37	X \$26 =	<b>962</b>	OR	X \$ =
	Independent (37 CFR 1.16(h))	* 6	Minus *** 3	= 3	X \$110 =	<b>330</b>	OR	X \$ =
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR	
					TOTAL ADD'L FEE	<b>1292</b>	OR	TOTAL ADD'L FEE

	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	X \$ =		OR	X \$ =
	Independent (37 CFR 1.16(h))	*	Minus ***	=	X \$ =		OR	X \$ =
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".  
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:  
 /JESSICA GAYNOR/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**  
 If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.





UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY. DOCKET NO, TOT CLAIMS, IND CLAIMS. Row 1: 12/720,147, 03/09/2010, 2183, 2052, ARAC-01RE1, 57, 6

CONFIRMATION NO. 8473

Allen F. Rozman
6402 Wildlife Trail
Garland, TX 75044

FILING RECEIPT



Date Mailed: 03/10/2010

Receipt is acknowledged of this reissue patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Applicant(s)

Allen F. Rozman, Garland, TX;
Alfonso J. Cioffi, Murphy, TX;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a REI of 10/913,609 08/07/2004 PAT 7,484,247

Foreign Applications

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

\*\* SMALL ENTITY \*\*

Title

SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE

Preliminary Class

712

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent

in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

## **LICENSE FOR FOREIGN FILING UNDER**

### **Title 35, United States Code, Section 184**

### **Title 37, Code of Federal Regulations, 5.11 & 5.15**

#### **GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY. DOCKET NO, TOT CLAIMS, IND CLAIMS. Row 1: 12/720,147, 03/09/2010, 2431, 2052, ARAC-01RE1, 57, 6

CONFIRMATION NO. 8473

REPLACEMENT FILING RECEIPT

Allen F. Rozman
6402 Wildlife Trail
Garland, TX 75044



Date Mailed: 03/11/2010

Receipt is acknowledged of this reissue patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Applicant(s)

Allen F. Rozman, Garland, TX;
Alfonso J. Cioffi, Murphy, TX;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a REI of 10/913,609 08/07/2004 PAT 7,484,247

Foreign Applications

If Required, Foreign Filing License Granted: 03/11/2010

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is US 12/720,147

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

\*\* SMALL ENTITY \*\*

**Title**

SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE

**Preliminary Class**

726

**PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

**LICENSE FOR FOREIGN FILING UNDER****Title 35, United States Code, Section 184****Title 37, Code of Federal Regulations, 5.11 & 5.15****GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where

the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

#### **NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

1 of 1 DOCUMENT

UNITED STATES PATENT AND TRADEMARK OFFICE GRANTED PATENT

7484247

[Link to Claims Section](#)

January 27, 2009

System and method for protecting a computer system from malicious , , software

**INVENTOR:** Rozman, Allen F - 735 Mockingbird Dr., Murphy, Texas, 75094, United States (US)Cioffi, Alfonso J - 719 Mockingbird Dr., Murphy, Texas, 75094, United States (US)

**APPL-NO:** 913609 (10)

**FILED-DATE:** August 7, 2004

**GRANTED-DATE:** January 27, 2009

**CORE TERMS:** malware, user, processor, network, memory, computer, computer system, video, interface, software, storage, display, logical process, configured, interactive, executing, internet, infection, window, data processor, operating systems, automatically, electronic, browser, communicatively, coupled, subsystem, session, stored, downloaded

**ENGLISH-ABST:**

In a computer system, a first electronic data processor is communicatively coupled to a first memory space and a second memory space. A second electronic data processor is communicatively coupled the second memory space and to a network interface device. The second electronic data processor is capable of exchanging data across a network of one or more computers via the network interface device. A video processor is adapted to combine video data from the first and second electronic data processors and transmit the combined video data to a display terminal for displaying the combined video data in a windowed format. The computer system is configured such that a malware program downloaded from the network and executing on the second electronic data processor is incapable of initiating access to the first memory space.

## No Documents Found

No documents were found for your search terms  
"7484247 or 7,484,247"

---

Click "Save this search as an Alert" to schedule your search to run in the future.

- OR -

Click "Edit Search" to return to the search form and modify your search.

### Suggestions:

- Check for spelling errors .
  - Remove some search terms.
  - Use more common search terms, such as those listed in "Suggested Words and Concepts"
  - Use a less restrictive date range.
- 

Save this Search as an Alert

Edit Search



[About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)

Copyright © 2010 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.



## No Documents Found

No documents were found for your search terms  
"7484247 or 7,484,247"

---

Click "Save this search as an Alert" to schedule your search to run in the future.

- OR -

Click "Edit Search" to return to the search form and modify your search.

### Suggestions:

- Check for spelling errors .
  - Remove some search terms.
  - Use more common search terms, such as those listed in "Suggested Words and Concepts"
  - Use a less restrictive date range.
- 

Save this Search as an Alert

Edit Search



[About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)  
Copyright © 2010 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

## No Documents Found

No documents were found for your search terms  
"7484247 or 7,484,247"

---

Click "Save this search as an Alert" to schedule your search to run in the future.

- OR -

Click "Edit Search" to return to the search form and modify your search.

### Suggestions:

- Check for spelling errors .
  - Remove some search terms.
  - Use more common search terms, such as those listed in "Suggested Words and Concepts"
  - Use a less restrictive date range.
- 

Save this Search as an Alert

Edit Search



[About LexisNexis](#) | [Terms & Conditions](#) | [Contact Us](#)

Copyright © 2010 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

[My Briefcase](#) | [Order Runner Documents](#) | [Available Courts](#) | [Learning Center](#)

**Single Search - with Terms and Connectors**

Enter keywords - Search multiple dockets & documents

**Search**

[View Demo](#)  
[Search Tips](#)

[My CourtLink](#)

[Search](#)

[Dockets & Documents](#)

[Track](#)

[Alert](#)

[Strategic Profiles](#)

[My Account](#)



[Search](#) > [Patent Search](#) > [Searching](#)

## Patent Search 7484247 3/25/2010

No cases found.

**Return to Search**

(Charges for search still apply)



[About LexisNexis](#) | [Terms & Conditions](#) | [Pricing](#) | [Privacy](#) | [Customer Support](#) - 1-888-311-19  
Copyright © 2010 LexisNexis®. All rights reserved.

File 670:LitAlert 1973-2010/UD=201012  
(c) 2010 Thomson Reuters

Set Items Description  
-----

**e pn=us 7484247**

Ref	Items	Index-term
E1	1	PN=US 7483524
E2	1	PN=US 7483592
E3	0	*PN=US 7484247
E4	1	PN=US 7484327
E5	1	PN=US 7484671
E6	3	PN=US 7484867
E7	3	PN=US 7485079
E8	1	PN=US 7485297
E9	1	PN=US 7485634
E10	1	PN=US 7486124

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number		12720147
	Filing Date		2010-03-09
	First Named Inventor	Rozman, Allen F.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		ARAC-01RE1

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	4890098	B2	1989-12-26	Dawes, et al		
	2	5280579	B2	1994-01-18	Nye		
	3	5502808	B2	1996-03-26	Goddard, et al		
	4	5555364	B2	1996-09-10	Goldstein		
	5	5666030	B2	1997-09-09	Parson		
	6	5673403	B2	1997-09-30	Brown, et al		
	7	5751979	B2	1998-05-12	McCroy		
	8	5826013	B2	1998-10-20	Nachenberg		

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		12720147
Filing Date		2010-03-09
First Named Inventor	Rozman, Allen F.	
Art Unit		
Examiner Name		
Attorney Docket Number		ARAC-01RE1

	9	5918039	B2	1999-06-29	Buswell, et al	
	10	5978917	B2	1999-11-02	Chi	
	11	5995103	B2	1999-11-30	Ashe	
	12	6134661	B2	2000-10-07	Topp	
	13	6167522	B2	2000-12-26	Lee, et al	
	14	6192477	B1	2001-02-20	Corthell	
	15	6199181	B1	2001-03-06	Rechef, et al	
	16	6216112	B1	2001-04-10	Fuller, et al	
	17	6275938	B1	2001-08-14	Bond, et al	
	18	6351816	B1	2002-02-26	Mueller, et al	
	19	6385721	B1	2002-05-07	Puckette	

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		12720147
Filing Date		2010-03-09
First Named Inventor	Rozman, Allen F.	
Art Unit		
Examiner Name		
Attorney Docket Number		ARAC-01RE1

	20	6480198	B1	2002-11-12	Kang	
	21	6507904	B1	2003-01-14	Ellison, et al	
	22	6507948	B1	2003-01-14	Curtis, et al	
	23	6546554	B1	2003-04-08	Schmidt, et al	
	24	6553377	B1	2003-04-22	Eschelbeck, et al	
	25	6578140	B1	2003-06-10	Policard	
	26	6581162	B1	2003-06-17	Angelo, et al	
	27	6633963	B1	2003-10-14	Ellison, et al	
	28	6658573	B1	2003-12-02	Bischof	
	29	6663000	B1	2003-12-16	Muttick, et al	
	30	6678825	B1	2004-01-13	Ellison, et al	

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number	12720147
Filing Date	2010-03-09
First Named Inventor	Rozman, Allen F.
Art Unit	
Examiner Name	
Attorney Docket Number	ARAC-01RE1

31	6735700	B1	2004-05-11	Flint, et al	
32	6321337	B1	2001-11-20	Rechef, et al	
33	7146640	B2	2006-12-05	Goodman, et al	
34	7260839	B2	2007-08-12	Karasaki	

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

**U.S.PATENT APPLICATION PUBLICATIONS**

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code <sup>1</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20020066016	A1	2002-05-12	Riordan	
	2	20020174349	A1	2002-11-21	Wolff, et al	
	3	20030023857	A1	2003-01-30	Hinchcliffe, et al	
	4	20030097591	A1	2003-05-22	Pham, et al	
	5	20030177397	A1	2003-09-18	Samman	



**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number	12720147
Filing Date	2010-03-09
First Named Inventor	Rozman, Allen F.
Art Unit	
Examiner Name	
Attorney Docket Number	ARAC-01RE1

6	20040006715	A1	2004-01-08	Skrepetos	
7	20040034794	A1	2004-02-19	Mayer, et al	
8	20040039944	A1	2004-02-26	Karasaki	
9	20040054588	A1	2004-03-18	Jacobs, et al	
10	20050240810	A1	2005-10-27	Safford, et al	
11	20060004667	A1	2006-01-05	Neil	

If you wish to add additional U.S. Published Application citation information please click the Add button.

**FOREIGN PATENT DOCUMENTS**

Examiner Initial*	Cite No	Foreign Document Number <sup>3</sup>	Country Code <sup>2</sup> i	Kind Code <sup>4</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T <sup>5</sup>
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button

**NON-PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>5</sup>

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number	12720147
	Filing Date	2010-03-09
	First Named Inventor	Rozman, Allen F.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	ARAC-01RE1

1	"Spyware, Adware, and Peer to Peer Networks; The Hidden Threat to Corporate Security" by KEVIN TOWNSEND, Pest Patrol, 2003	<input type="checkbox"/>
2	"Beyond Viruses: Why Anti-Virus Software is No Longer Enough" by DAVID STANG PhD, Pest Patrol, 2002	<input type="checkbox"/>
3	"The Web: Threat or Menace?" from "Firewalls and Internet Security: Repelling the Wiley Hacker", Second Edition, Addison-Wesley, ISBN 0-201-63466-X, 2003	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

**EXAMINER SIGNATURE**

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> See Kind Codes of USPTO Patent Documents at [www.USPTO.GOV](http://www.USPTO.GOV) or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>3</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>4</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here if English language translation is attached.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number	12720147
	Filing Date	2010-03-09
	First Named Inventor	Rozman, Allen F.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	ARAC-01RE1

**CERTIFICATION STATEMENT**

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

**OR**

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

None

**SIGNATURE**

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/A. F. Rozman/	Date (YYYY-MM-DD)	2010-03-09
Name/Print	Allen F. Rozman	Registration Number	41280

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

## Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number		12720147
	Filing Date		2010-03-09
	First Named Inventor	Rozman et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		ARAC-01RE1

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	5673403	B2	1997-09-30	Brown, et al		
	2	5751979	B2	1998-05-12	McCrory		
	3	5974549	B2	1999-10-26	Golan		
	4	5978917	B2	1999-11-02	Chi		
	5	6091412	B2	2000-07-18	Simonoff, et al		
	6	6134661	B2	2000-10-17	Topp		
	7	6397242	B1	2002-05-28	Devine, et al		
	8	6401134	B1	2002-06-04	Razavi, et al		

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		12720147
Filing Date		2010-03-09
First Named Inventor	Rozman et al.	
Art Unit		
Examiner Name		
Attorney Docket Number		ARAC-01RE1

	9	6433794	B1	2002-08-09	Beadle, et al	
	10	6438600	B1	2002-08-20	Greenfield, et al	
	11	6492995	B1	2002-12-10	Atkin, et al	
	12	6678825	B1	2004-01-13	Ellison, et al	
	13	6691230	B1	2004-02-10	Bardon	
	14	6757685	B1	2004-06-29	Rafaelle, et al	
	15	6836885	B1	2004-12-28	Buswell, et al	
	16	7024555	B1	2006-04-06	Kozuch, et al	
	17	7139890	B1	2006-11-21	Moran, et al	
	18	7146640	B1	2006-12-05	Goodman, et al	
	19	7260839	B1	2007-08-21	Karasaki	

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number	12720147
Filing Date	2010-03-09
First Named Inventor	Rozman et al.
Art Unit	
Examiner Name	
Attorney Docket Number	ARAC-01RE1

20	7401230	B1	2008-08-15	Campbell, et al	
21	7421689	B1	2008-09-02	Ross, et al	
22	7565522	B1	2009-07-21	Sastry, et al	

If you wish to add additional U.S. Patent citation information please click the Add button.

**U.S.PATENT APPLICATION PUBLICATIONS**

Examiner Initial*	Cite No	Publication Number	Kind Code <sup>1</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

**FOREIGN PATENT DOCUMENTS**

Examiner Initial*	Cite No	Foreign Document Number <sup>3</sup>	Country Code <sup>2</sup> ;	Kind Code <sup>4</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T <sup>5</sup>
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button

**NON-PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>5</sup>
	1	Architecture of Virtual Machines by R. P. GOLDBERG, Honeywell Information Systems, Inc. and Harvard University presented at the AFIPS National Computer Conference, New York, New York, June 4-8, 1973.	<input type="checkbox"/>

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number	12720147
Filing Date	2010-03-09
First Named Inventor	Rozman et al.
Art Unit	
Examiner Name	
Attorney Docket Number	ARAC-01RE1

2	The Duality of Memory and Communication in the Implementation of a Multiprocessor Operating System by MICHAEL YOUNG, AVADIS TEVANIAN, RICHARD RASHEED, DAVID GOLUB, JEFFERY EPPINGER, JONATHAN CREW, WILLIAM BOLOSKY, DAVID BLACK and ROBERT BARON, Computer Science Department Carnegie-Mellon University Appeared in Proceedings of the 11th Operating Systems Principles, November, 1987	<input type="checkbox"/>
3	Application-Controlled Physical Memory using External Page-Cache Management by KEIRAN HARTY and DAVID R. CHERITON, Computer Science Department, Stanford University, 1992	<input type="checkbox"/>
4	Efficient Software-Based Fault Isolation by ROBERT WAHBE, STEVEN LUCCO, THOMAS ANDERSON, SUSAN GRAHAM, Computer Science Division University of California, Berkeley, SIGOPS 1993	<input type="checkbox"/>
5	TRON: Process-Specific File Protection for the UNIX Operating System by ANDREW BERMAN, VIRGIL BOURASSA, ERIK SELBERG, Department of Computer Science and Engineering, University of Washington, January 23, 1995	<input type="checkbox"/>
6	A Secure Environment for Untrusted Helper Applications (Confining the Wily Hacker) by IAN GOLDBERG, DAVID WAGNER, RANDI THOMAS, and ERIC BREWER, Computer Science Division, University of California, Berkeley, Sixth USENIX UNIX Security Symposium San Jose, California, July 1996	<input type="checkbox"/>
7	Building Systems that Flexibly Control Downloaded Executable Context by TRENT JAEGER and ATUL PRAKASH, Software Systems Research Lab, University of Michigan and AVIEL D. RUBIN, Security Research Group, Bellcore Sixth USENIX UNIX Security Symposium San Jose, California, July 1996	<input type="checkbox"/>
8	Java Security: From HotJava to Netscape and Beyond by DREW DEAN, EDWARD W. FELTEN, DAN S. WALLACH Department of Computer Science, Princeton University, Princeton, NJ 08544 1996 IEEE Symposium on Security and Privacy, Oakland, CA, May 6-8, 1996.	<input type="checkbox"/>
9	ChakraVyuha (CV) : A Sandbox Operating System Environment for Controlled Execution of Alien Code by ASIT DAN, AJAY MOHINDRA, RAJIV RAMASWAMI, and DINKAR SITARAM IBM Research Division T.J. Watson Research Center Yorktown Heights, New York RC 20742 (2/20/97) Computer Science IBM Research Report LIMITED DISTRIBUTION	<input type="checkbox"/>
10	Vulnerability of Secure Web Browsers by FLAVIO DE PAOLI, ANDRE DOS SANTOS, RICHARD KEMMERER Reliable Software Group Computer Science Department, University of California, Santa Barbara, 1997	<input type="checkbox"/>
11	Security of Web Browser Scripting Languages: Vulnerabilities, Attacks, and Remedies by VINOD ANUPAM and ALAIN MAYER, Bell Laboratories, Lucent Technologies 7th USENIX Security Symposium San Antonio, Texas, January 26-29, 1998	<input type="checkbox"/>
12	"Virtual Memory in Contemporary Microprocessors" by BRUCE JACOB University of Maryland and TREVOR MUDGE University of Michigan, IEEE MICRO JULY-AUGUST 1998	<input type="checkbox"/>



**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		12720147
Filing Date		2010-03-09
First Named Inventor	Rozman et al.	
Art Unit		
Examiner Name		
Attorney Docket Number	ARAC-01RE1	

13	"Flexible Control of Downloaded Executable Content" by TRENT JAEGER and JOCHEN LIEDTKE and NAYEEM ISLAM, IBM Thomas J. Watson Research Center, and ATUL PRAKASH University of Michigan, Ann Arbor ACM Transactions on Information and System Security, Vol. 2, No. 2, May 1999, Pages 177–228.	<input type="checkbox"/>
14	"J2ME Building Blocks for Mobile Devices: White Paper on KVM and the Connected", Limited Device Configuration Sun Microsystems May 19, 2000	<input type="checkbox"/>
15	"User-level Resource-constrained Sandboxing" by FANGZHE CHANG, AYAL ITZKOVITZ, and VIJAY KARAMCHETI Department of Computer Science, Courant Institute of Mathematical Sciences, New York University USENIX Windows System Symposium, August 2000	<input type="checkbox"/>
16	"Verifying the EROS Confinement Mechanism" by JONATHAN S. SHAPIRO and SAN WEBER IBM T.J. Watson Research Center 0-7695-0665-8/00 2000 IEEE	<input type="checkbox"/>
17	"WindowBox: A Simple Security Model for the Connected Desktop" by DIRK BALFANZ, Princeton University and DANIEL R. SIMON, Microsoft Research, 2000	<input type="checkbox"/>
18	"Building a Secure Web Browser" by SOTIRIS IOANNIDIS, University of Pennsylvania, and STEVEN M. BELLOVIN, AT&T Labs Research 2001 USENIX Annual Technical Conference Boston, Massachusetts, USA June 25–30, 2001	<input type="checkbox"/>
19	"Virtualizing I/O Devices on VMware Workstation's Hosted Virtual Machine Monitor" by JEREMY SUGERMAN, GANESH VENKITACHALAM and BENG-HONG LIM, VMware, Inc. 3145 Porter Dr, Palo Alto, CA 943042001 USENIX Annual Technical Conference Boston, Massachusetts, USA June 25–30, 2001	<input type="checkbox"/>
20	"When Virtual Is Better Than Real" by PETER M. CHEN and BRIAN D. NOBLE, Department of Electrical Engineering and Computer Science University of Michigan 2001	<input type="checkbox"/>
21	"A Flexible Containment Mechanism for Executing Untrusted Code" by DAVID PETERSON, MATT BISHOP, and RAJU PANDEY, Department of Computer Science University of California, Davis USENIX Security Symposium San Francisco, California, USA August 5-9, 2002	<input type="checkbox"/>
22		<input type="checkbox"/>
23	"ReVirt: Enabling Intrusion Analysis through Virtual-Machine Logging and Replay" by GEORGE W. DUNLAP, SAMUEL T. KING, SUKRU CINAR, MURTAZA A. BASRAI, PETER M. CHEN, Department of Electrical Engineering and Computer Science, University of Michigan Proceedings of the 2002 Symposium on Operating Systems Design and Implementation (OSDI)	<input type="checkbox"/>

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		12720147
Filing Date		2010-03-09
First Named Inventor	Rozman et al.	
Art Unit		
Examiner Name		
Attorney Docket Number	ARAC-01RE1	

24	"Trusted Paths for Browsers: An Open-Source Solution to Web Spoofing" by ZISHUANG (Eileen) YE and SEAN SMITH Department of Computer Science Dartmouth College Technical Report TR2002-418 February 4, 2002	<input type="checkbox"/>
25	"User Interaction Design for Secure Systems" by KA-PING YEE <a href="http://zesty.ca/sid/">http://zesty.ca/sid/</a> 2002	<input type="checkbox"/>
26	BAA-00-06-SNK Focused Research Topic 5 by MARC STIEGLER AND MARK MILLER Report Name: "A Capability Based Client: The DarpaBrowser" 26 June 2002	<input type="checkbox"/>
27	"A Virtual Machine Introspection Based Architecture for Intrusion Detection" by TAL GARFINKEL and MENDEL ROSENBLUM, Computer Science Department, Stanford University 2003	<input type="checkbox"/>
28	"Terra: A Virtual Machine-Based Platform for Trusted Computing" by TAL GARFINKEL, BEN PFAFF, JIM CHOW, DAN BONEH and MENDEL ROSENBLUM, Computer Science Department, Stanford University SOSP'03, October 19-22, 2003, Bolton Landing, New York, USA.	<input type="checkbox"/>
29	Microsoft® Virtual PC 2004 Technical Overview by JERRY HONEYCUTT Published November 2003 <a href="http://download.microsoft.com/download/c/f/b/cfb100a7-463d-4b86-ad62-064397178b4f/Virtual_PC_Technical_Overview.doc">http://download.microsoft.com/download/c/f/b/cfb100a7-463d-4b86-ad62-064397178b4f/Virtual_PC_Technical_Overview.doc</a>	<input type="checkbox"/>
30	"Xen and the Art of Virtualization" by PAUL BARHAM, BORIS DRAGOVIC, KEIR FRASER, STEVEN HAND, TIM HARRIS, ALEX HO, ROLF NEUGEBAUREY, IAN PRATT, ANDREW WARFIELD University of Cambridge Computer Laboratory 15 JJ Thomson Avenue, Cambridge, UK, CB3 0FD SOSP'03, October 19-22, 2003, Bolton Landing, New York, USA	<input type="checkbox"/>
31	"Design of the EROS Trusted Window System" by JONATHAN S. SHAPIRO, JOHN VANDERBURGH, ERIC NORTHROP, Systems Research Laboratory Johns Hopkins University, and, DAVID CHIZMADIA, Promia, Inc. 2004	<input type="checkbox"/>
32	"Survey of System Virtualization" Techniques by ROBERT ROSE March 8, 2004	<input type="checkbox"/>
33	White Paper: "Smart Phone Security Issues" by LUC DELPHA and MALIHA RASHEED, Cyber Risk Consulting Blackhat Briefings Europe May 2004	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number	12720147
	Filing Date	2010-03-09
	First Named Inventor	Rozman et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	ARAC-01RE1

**EXAMINER SIGNATURE**

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> See Kind Codes of USPTO Patent Documents at [www.USPTO.GOV](http://www.USPTO.GOV) or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>3</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>4</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here if English language translation is attached.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number	12720147
	Filing Date	2010-03-09
	First Named Inventor	Rozman et al.
	Art Unit	
	Examiner Name	
	Attorney Docket Number	ARAC-01RE1

**CERTIFICATION STATEMENT**

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

**OR**

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

None

**SIGNATURE**

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/A. F. Rozman/	Date (YYYY-MM-DD)	
Name/Print	Allen F. Rozman	Registration Number	41280

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

## Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	12720147
<b>Filing Date:</b>	09-Mar-2010
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Filer:</b>	Glenn W. Boisbrun
<b>Attorney Docket Number:</b>	ARAC-01RE1

Filed as Large Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
Submission- Information Disclosure Stmt	1806	1	180	180
<b>Total in USD (\$)</b>				<b>180</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	7414443
<b>Application Number:</b>	12720147
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	8473
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Correspondence Address:</b>	Allen F. Rozman - 6402 Wildlife Trail - Garland TX 75044 US 214-478-2172 arozman@verizon.net
<b>Filer:</b>	Glenn W. Boisbrun
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	ARAC-01RE1
<b>Receipt Date:</b>	14-APR-2010
<b>Filing Date:</b>	09-MAR-2010
<b>Time Stamp:</b>	17:09:50
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$180



RAM confirmation Number		13429			
Deposit Account					
Authorized User					
<b>File Listing:</b>					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	ARAC-01RE1_IDS.pdf	1158349	no	8
			e1f8f9cb3cb53cf88d586da6a8e5d7dbac91bc7c		
<b>Warnings:</b>					
<b>Information:</b>					
2	Information Disclosure Statement (IDS) Filed (SB/08)	ARAC-01RE1_IDS_Supp.pdf	1251976	no	9
			2998671bb53ac21315ccca3d3a287612ecd4dd482		
<b>Warnings:</b>					
<b>Information:</b>					
3	NPL Documents	NPL_3.pdf	43422	no	6
			3c5bb6e3ed801fa145d88ffda962715d34766855		
<b>Warnings:</b>					
<b>Information:</b>					
4	NPL Documents	NPL_4.pdf	167404	no	20
			0248b821ce48d6bed575c2bdaecc63e8e7f78aa8		
<b>Warnings:</b>					
<b>Information:</b>					
5	NPL Documents	NPL_5.pdf	87999	no	14
			34d1effe1c66c3b0285379786c382201d22d1526		
<b>Warnings:</b>					
<b>Information:</b>					
6	NPL Documents	NPL_6.pdf	83405	no	11
			e2f2d4af8740ec38d2f308c353e1d501ed2b28e		
<b>Warnings:</b>					
<b>Information:</b>					
7	NPL Documents	NPL_7.pdf	230060	no	21
			68cb36acd8bcb73fc6e65dde5e005c9b252df0		
<b>Warnings:</b>					
<b>Information:</b>					
8	NPL Documents	NPL_8.pdf	606663	no	101
			ccca17fa03099b8ed85993304a1b8146e8b26d2d		

<b>Warnings:</b>					
<b>Information:</b>					
9	NPL Documents	NPL_9.pdf	179689 645751a1520d46eb7acda9436f27091d2c71bb52	no	9
<b>Warnings:</b>					
<b>Information:</b>					
10	NPL Documents	NPL_10.pdf	149817 c8b135504d72c330d024cdbffe50d130ec0b2c94	no	14
<b>Warnings:</b>					
<b>Information:</b>					
11	NPL Documents	NPL_11.pdf	98453 67a71d285710bc9a176f468570dffa44996fd438	no	16
<b>Warnings:</b>					
<b>Information:</b>					
12	NPL Documents	NPL_12.pdf	1844837 ea47559f02b467a9c74ae78f4a4f9c20b8d54b87	no	27
<b>Warnings:</b>					
<b>Information:</b>					
13	NPL Documents	NPL_13.pdf	297660 df3ce3bf192828c86cd14a0e014d7cf626c05708	no	14
<b>Warnings:</b>					
<b>Information:</b>					
14	NPL Documents	NPL_14.pdf	296286 72a42c4eaf749bb238096af3c1dbcb8259725b7	no	12
<b>Warnings:</b>					
<b>Information:</b>					
15	NPL Documents	NPL_18.pdf	137498 32bd86ae539c547b3eaaecb0a3751059b43ff883	no	15
<b>Warnings:</b>					
<b>Information:</b>					
16	NPL Documents	NPL_19.pdf	2476000 60a3daffff5638a6c969a0c6ecb6a15373dbc44	no	39
<b>Warnings:</b>					
<b>Information:</b>					
17	NPL Documents	NPL_20.pdf	61583 f3ae1b93e271e41c4617a082f0e70125a29	no	23

<b>Warnings:</b>					
<b>Information:</b>					
18	NPL Documents	NPL_21.pdf	195205 a0612533089d356bce4b07e2d11de5d8f7fae143	no	11
<b>Warnings:</b>					
<b>Information:</b>					
19	NPL Documents	NPL_22.pdf	1485312 7d28b133f3ed54aa29947421deabddf65b8c586d	no	14
<b>Warnings:</b>					
<b>Information:</b>					
20	NPL Documents	NPL_23.pdf	132479 4de82737f5a6d3a10a2ac58564c15ec432044d81	no	16
<b>Warnings:</b>					
<b>Information:</b>					
21	NPL Documents	NPL_24.pdf	254873 27c20a89db009126c9077ffa57e9ca5e5f65b3bc	no	14
<b>Warnings:</b>					
<b>Information:</b>					
22	NPL Documents	NPL_25.pdf	314762 b917848087009642a9d2099c15371621ec5db367	no	19
<b>Warnings:</b>					
<b>Information:</b>					
23	NPL Documents	NPL_26.pdf	114005 83dbde681c1401fa203e05146c19d797434609d9	no	11
<b>Warnings:</b>					
<b>Information:</b>					
24	NPL Documents	NPL_28.pdf	210035 3b0c4a556edc6cccf49f6edb8f9f7310d87c17b0	no	12
<b>Warnings:</b>					
<b>Information:</b>					
25	NPL Documents	NPL_30.pdf	232266 d0a7762c9e1f016fd9316153b16ad553c640486f	no	16
<b>Warnings:</b>					
<b>Information:</b>					
26	NPL Documents	NPL_31.pdf	283370 19634064865cf483e1c27a053095457600	no	52

<b>Warnings:</b>					
<b>Information:</b>					
27	NPL Documents	NPL_34.pdf	163014 58b4219acf9e5d53578a45f21e74c67dc70be88b	no	11
<b>Warnings:</b>					
<b>Information:</b>					
28	NPL Documents	NPL_35.pdf	103620 1c04998328adb60559df0f4555539a02f16fb627	no	12
<b>Warnings:</b>					
<b>Information:</b>					
29	NPL Documents	NPL_16_.pdf	256857 2aa4aefad276be3dc91a6f827e4d2d9d34cecf9d	no	14
<b>Warnings:</b>					
<b>Information:</b>					
30	NPL Documents	NPL_27_.pdf	207130 ddfc3edbb3c9d3a10a833adc25432be698fdc7ed	no	23
<b>Warnings:</b>					
<b>Information:</b>					
31	NPL Documents	NPL_32_.pdf	373115 30893711f598b2ebf7e86cb5118e4848ed86469	no	42
<b>Warnings:</b>					
<b>Information:</b>					
32	NPL Documents	NPL_33_.pdf	189187 6a601c30ba5504b39ab814070d85ebb6564ce610	no	11
<b>Warnings:</b>					
<b>Information:</b>					
33	NPL Documents	NPL_1.pdf	551259 31cd9dd2a1d178065c569b2069958dccc6c9df9f9	no	9
<b>Warnings:</b>					
<b>Information:</b>					
34	NPL Documents	NPL_2.pdf	1539038 af87270a1e693561a90b1be46f7a2925ef5ae19a	no	15
<b>Warnings:</b>					
<b>Information:</b>					
35	NPL Documents	NPL_15.pdf	366100 1dd798290bc8bde5e11375e2agab14d706	no	5

<b>Warnings:</b>					
<b>Information:</b>					
36	NPL Documents	NPL_17.pdf	1428408 5e263942daae6216e5cd93e3f70fbd3ac31dfcc7	no	15
<b>Warnings:</b>					
<b>Information:</b>					
37	NPL Documents	NPL_29.pdf	1227102 a7922d5b5d0ba2af88cb4bf91e86cd175d0baed	no	14
<b>Warnings:</b>					
<b>Information:</b>					
38	Fee Worksheet (PTO-875)	fee-info.pdf	30357 bace2265ea70d1e9417611e0e11c7e7bd32725a4	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			18828595		

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number		12720147
	Filing Date		2010-03-09
	First Named Inventor	Rozman et al.	
	Art Unit	2439	
	Examiner Name	LAFORGIA, CHRISTIAN A	
	Attorney Docket Number	ARAC-01RE1	

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	6880110	B2	2005-04-12	Largman et al.		
	2	7096381	B2	2006-08-22	Largman et al.		
	3	7577871	B2	2009-08-18	Largman et al.		
	4	7694328		2010-04-06	Joshi et al.		
	5	7373505	B2	2008-05-13	Seltzer et al.		
	6	7039801	B2	2006-05-02	Narin		
	7	7596694	B1	2009-09-29	Karp et al.		
	8	7085928	B1	2006-08-01	Schmid et al.		

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		12720147
Filing Date		2010-03-09
First Named Inventor	Rozman et al.	
Art Unit		2439
Examiner Name	LAFORGIA, CHRISTIAN A	
Attorney Docket Number		ARAC-01RE1

	9	7181768	B1	2007-02-20	Ghosh et al.	
	10	7284274	B1	2007-10-16	Walls et al.	
	11	6804780	B1	2004-10-12	Touboul	
	12	7191469	B2	2007-03-13	Erlingsson	
	13	6505300	B2	2003-01-07	Chan et al.	
	14	7246374	B1	2007-07-17	Simon et al.	
	15	7062672	B2	2006-06-13	Owhadi et al.	
	16	7444412	B2	2008-10-28	Owhadi	
	17	6772345	B1	2004-08-03	Shetty	
	18	6108715		2000-08-22	Leach et al.	
	19	6873988	B2	2005-03-25	Herrmann et al.	

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number	12720147
	Filing Date	2010-03-09
	First Named Inventor	Rozman et al.
	Art Unit	2439
	Examiner Name	LAFORGIA, CHRISTIAN A
	Attorney Docket Number	ARAC-01RE1

If you wish to add additional U.S. Patent citation information please click the Add button.

**U.S.PATENT APPLICATION PUBLICATIONS**

Examiner Initial*	Cite No	Publication Number	Kind Code <sup>1</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030131152		2003-07-10	Ulfar Erlingsson	

If you wish to add additional U.S. Published Application citation information please click the Add button.

**FOREIGN PATENT DOCUMENTS**

Examiner Initial*	Cite No	Foreign Document Number <sup>3</sup>	Country Code <sup>2</sup> j	Kind Code <sup>4</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T <sup>5</sup>
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button

**NON-PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>5</sup>
	1	"SOFTWARE SECURITY AND PRIVACY RISKS IN MOBILE E-COMMERCE" by Anup K. Ghosh and Tara M. Swaminatha, COMMUNICATIONS OF THE ACM February 2001 Vol. 44, No. 2	<input type="checkbox"/>
	2	T. Jaeger, A. D. Rubin, and A. Prakash. "Building systems that flexibly control downloaded executable content." In Proceedings of the 1996 USENIX Security Symposium, pages 131-148, San Jose, Ca., 1996.	<input type="checkbox"/>
	3	Nimisha V. Mehta, Karen R. Sollins, "Expanding and Extending the Security Features of Java." Proceedings of the 7th USENIX Security Symposium, San Antonio, Texas, January 26-29, 1998	<input type="checkbox"/>
	4	David A. Wagner, "Janus: an approach for confinement of untrusted applications." Master's thesis, University of California, Berkeley, 1999.. Also available, Technical Report CSD-99-1056, UC Berkeley, Computer Science Division. <a href="http://www.cs.berkeley.edu/~daw/papers/janus-masters.ps">http://www.cs.berkeley.edu/~daw/papers/janus-masters.ps</a>	<input type="checkbox"/>



**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		12720147
Filing Date		2010-03-09
First Named Inventor	Rozman et al.	
Art Unit	2439	
Examiner Name	LAFORGIA, CHRISTIAN A	
Attorney Docket Number	ARAC-01RE1	

5	Richard West and Jason Gloudon, "User-Level Sandboxing: a Safe and Efficient Mechanism for Extensibility", Technical Report, 2003-014, Boston University, June 2003	<input type="checkbox"/>
6	Shaya Potter, Jason Nieh, Dinesh Subhraveti, "Secure Isolation and Migration of Untrusted Legacy Applications." Columbia University Technical Report CUCS-005-04, January 2004	<input type="checkbox"/>
7	M. Schmid, F. Hill, A. Ghosh, "Protecting Data from Malicious Software." Annual Computer Security Applications Conference (ACSAC'02), Las Vegas, NV, December, 2002.	<input type="checkbox"/>
8	Valentin Razmov "Security in Untrusted Code Environments: Missing Pieces of the Puzzle." Dept. of Computer Science and Engineering, University of Washington, March 30, 2002	<input type="checkbox"/>
9	Sotiris Ioannidis and Steven M. Bellovin. "Sub-Operating Systems: A New Approach to Application Security." Technical Report MS-CIS-01-06, University of Pennsylvania, February 2000.	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

**EXAMINER SIGNATURE**

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> See Kind Codes of USPTO Patent Documents at [www.USPTO.GOV](http://www.USPTO.GOV) or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>3</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>4</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number	12720147
Filing Date	2010-03-09
First Named Inventor	Rozman et al.
Art Unit	2439
Examiner Name	LAFORGIA, CHRISTIAN A
Attorney Docket Number	ARAC-01RE1

**CERTIFICATION STATEMENT**

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

**OR**

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

None

**SIGNATURE**

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/A. F. Rozman/	Date (YYYY-MM-DD)	2010-08-05
Name/Print	Allen F. Rozman	Registration Number	41280

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

## Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	8164562
<b>Application Number:</b>	12720147
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	8473
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Correspondence Address:</b>	Allen F. Rozman - 6402 Wildlife Trail - Garland TX 75044 US 214-478-2172 arozman@verizon.net
<b>Filer:</b>	Allen Frank Rozman
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	ARAC-01RE1
<b>Receipt Date:</b>	05-AUG-2010
<b>Filing Date:</b>	09-MAR-2010
<b>Time Stamp:</b>	16:50:09
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	ARAC_01RE1_12720147_IDS_Supplemental_8_5_2010.pdf	614019 a7aedab43f0542f27f09a112b038e174b0e3216b	no	6
<b>Warnings:</b>					
<b>Information:</b>					
2	NPL Documents	1998_Expanding_and_Extending_the_Security_Features_of_Java.pdf	5406 a387fad81af1ae9aa3dc867faf5b69b62a198c2	no	2
<b>Warnings:</b>					
<b>Information:</b>					
3	NPL Documents	1999_Janus_an_approach_for_confinement_of_untrusted_applications.pdf	562929 c449a2eccc906cee923c905409234073ce95468	no	65
<b>Warnings:</b>					
<b>Information:</b>					
4	NPL Documents	2001_SOFTWARE_SECURITY_AND_PRIVACY_RISKS.pdf	89043 7aa5a7b82990e659e11476622a698287948bd156	no	7
<b>Warnings:</b>					
<b>Information:</b>					
5	NPL Documents	2002_Protecting_Data_from_Malicious_Software.pdf	243320 a0354c904c618aecb1f7d79e57d468f64aa738b2	no	10
<b>Warnings:</b>					
<b>Information:</b>					
6	NPL Documents	2002_Security_in_Untrusted_Code_Environments_Missing_Pieces_of_the_Puzzle.pdf	391797 57826f637a560ec64be8d120395949efead267ed	no	22
<b>Warnings:</b>					
<b>Information:</b>					
7	NPL Documents	2002_Sub_Operating_Systems_A_New_Approach_to_Application_Security.pdf	116179 7c98b7516e0bcff8b5335c8c0ad4426215edc7145	no	9
<b>Warnings:</b>					
<b>Information:</b>					
8	NPL Documents	2003_User_Level_Sandboxing_a_Safe_and_Efficient_Mechanism_for_Extensibility.pdf	192505 86fc9e90f93f9421991a97e0b82ae27c41821b89	no	13
<b>Warnings:</b>					
<b>Information:</b>					
9	NPL Documents	2004_Secure_Isolation_and_Migration_of_Untrusted_Legacy_Applications.pdf	165993 6ab1abe158a479573a520a127387c59ede22dcdd	no	16

<b>Warnings:</b>					
<b>Information:</b>					
10	NPL Documents	1996_Building_systems_that_f exibly_control_downloaded_e xecutable_content.pdf	1359844	no	19
			7a4fbbd000dc5044bc10c3cca676efbf1243 cbae		
<b>Warnings:</b>					
<b>Information:</b>					
			<b>Total Files Size (in bytes):</b>	3741035	
<p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  <b>If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</b></p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  <b>If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</b></p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  <b>If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</b></p>					

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicants:	Rozman, <i>et al.</i>	Docket No.:	ARAC-01RE1
Serial No.:	12720147	Filed:	09-MAR-2010
Reissue of:	7,484,247	Issued:	27-JAN-2009
Title:	System and Method for Protecting a Computer System from Malicious Software.		

Mail Stop: REISSUE  
Commissioner for Patents  
P. O. Box 1450  
Alexandria, VA 22313-1450

**SUPPLEMENTAL PRELIMINARY AMENDMENT**

Dear Sir:

Prior to examination on the merits, Applicants respectfully submit the amendments and remarks set forth below.

In the Specification:

Please delete the following material from the previous Preliminary Amendment, filed on 09-MAR-2010:

~~This application is a reissue application of U.S. Patent No. 7,484,247, entitled “System and Method for Protecting a Computer System from Malicious Software,” issued on January 27, 2009, and is related to another reissue application designated U.S. Patent Application Serial No. \_\_\_\_\_ (Docket No. ARAC 01RE2) from U.S. Patent No. 7,484,247 filed concurrently herewith, which are incorporated herein by reference.~~

Before the heading “Cross Reference to Related Patents and Applications” please insert:

Cross Reference to Multiple Reissue Applications

This application is a reissue application of U.S. Patent No. 7,484,247, entitled “System and Method for Protecting a Computer System from Malicious Software,” issued on 27-JAN-2009, and is related to reissue application designated U.S. Patent Application Serial No. 12720207, (Docket No. ARAC-01RE2) from U.S. Patent No. 7,484,247, filed on 09-MAR-2010, and is also related to reissue application designated U.S. Patent Application Serial No. 12854149, (Docket No. ARAC-01RE3) from U.S. Patent No. 7,484,247, filed on 10-AUG-2010, and is also related to reissue application designated U.S. Patent Application Serial No. 12941067, (Docket No. ARAC-01RE4) from U.S. Patent No. 7,484,247, filed on 07-NOV-2010. The above reissue applications are incorporated herein by reference in their entirety.



**REMARKS**

Please enter the above amendments before consideration of this application. The Applicants believe the claims are in condition for allowance and respectfully request that the Examiner pass the case to reissuance. The Examiner is invited to contact the undersigned to address any questions or concerns regarding the present reissue application.

Respectfully submitted,

13-NOV-2010

Date

/A. F. Rozman/

Allen F. Rozman  
Co-Applicant  
Registered Patent Agent  
Reg. No. 41,280

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	8831961
<b>Application Number:</b>	12720147
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	8473
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Correspondence Address:</b>	Allen F. Rozman - 6402 Wildlife Trail - Garland TX 75044 US 214-478-2172 arozman@verizon.net
<b>Filer:</b>	Allen Frank Rozman
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	ARAC-01RE1
<b>Receipt Date:</b>	13-NOV-2010
<b>Filing Date:</b>	09-MAR-2010
<b>Time Stamp:</b>	12:36:39
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Supplemental Response or Supplemental Amendment	ARAC-01RE1_Supplemental_Preliminary_Amendment.pdf	19600 0acc7331f091f1e5cd8ba859bfeb52170b8ab6c8	no	3

**Warnings:**

**Information:**

**Total Files Size (in bytes):** 19600

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
12/720,147 03/09/2010 Allen F. Rozman ARAC-01RE1 8473

7590 01/04/2011
Allen F. Rozman
6402 Wildlife Trail
Garland, TX 75044

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT PAPER NUMBER

2439

MAIL DATE DELIVERY MODE

01/04/2011

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 12/720,147	<b>Applicant(s)</b> ROZMAN ET AL.	
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1)  Responsive to communication(s) filed on 09 March 2010.
- 2a)  This action is **FINAL**.
- 2b)  This action is non-final.
- 3)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4)  Claim(s) 1-57 is/are pending in the application.
  - 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5)  Claim(s) \_\_\_\_\_ is/are allowed.
- 6)  Claim(s) 1-57 is/are rejected.
- 7)  Claim(s) \_\_\_\_\_ is/are objected to.
- 8)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9)  The specification is objected to by the Examiner.
- 10)  The drawing(s) filed on 09 March 2010 is/are: a)  accepted or b)  objected to by the Examiner.
  - Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
  - Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a)  All    b)  Some \*    c)  None of:
    - 1.  Certified copies of the priority documents have been received.
    - 2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    - 3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1)  Notice of References Cited (PTO-892)
- 2)  Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3)  Information Disclosure Statement(s) (PTO/SB/08)
  - Paper No(s)/Mail Date 4/14/10.
- 4)  Interview Summary (PTO-413)
  - Paper No(s)/Mail Date. \_\_\_\_\_.
- 5)  Notice of Informal Patent Application
- 6)  Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. Claims 1-57 have been presented for examination.

#### **Information Disclosure Statement**

2. The information disclosure statements (IDS) submitted on 14 April 2010 and 05 August 2010 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements have been considered by the examiner.

3. The information disclosure statement filed 05 August 2010 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. A copy of "Expanding and Extending the Security Features of Java" does not appear in the file (item #3 under "Non-Patent Literature Documents").

#### **Reissue Applications**

4. Claims 1-57 are rejected under 35 U.S.C. 251 as being improperly broadened in a reissue application made and sworn to by the assignee and not the patentee. A claim is broader in scope than the original claims if it contains within its scope any conceivable product or process which would have infringed the original patent. A claim is broadened if it is broader in any one respect even though it may be narrower in other respects.

5. Claims 1-57 are rejected under 35 U.S.C. 251 as being an improper recapture of broadened claimed subject matter surrendered in the application for the patent upon which the present reissue is based. See *Pannu v. Storz Instruments Inc.*, 258 F.3d 1366, 59 USPQ2d 1597 (Fed. Cir. 2001); *Hester Industries, Inc. v. Stein, Inc.*, 142 F.3d 1472, 46 USPQ2d 1641 (Fed. Cir. 1998); *In re Clement*, 131 F.3d 1464, 45 USPQ2d 1161 (Fed. Cir. 1997); *Ball Corp. v.*

Art Unit: 2439

United States, 729 F.2d 1429, 1436, 221 USPQ 289, 295 (Fed. Cir. 1984). A broadening aspect is present in the reissue which was not present in the application for patent. The record of the application for the patent shows that the broadening aspect (in the reissue) relates to claim subject matter that applicant previously surrendered during the prosecution of the application. Accordingly, the narrow scope of the claims in the patent was not an error within the meaning of 35 U.S.C. 251, and the broader scope of claim subject matter surrendered in the application for the patent cannot be recaptured by the filing of the present reissue application.

6. North American Container, Inc. v. Plastipak Packaging, Inc., 415 F.3d 1335, 75 USPQ2d 1545 (Fed. Cir. 2005) reiterated a three step test for determining whether recapture exists. MPEP § 1412.02(I). To determine whether recapture exists, a determination must be made whether the reissue claims are broader in scope than the original patent claims. Next, the reissue claims must be analyzed to determine whether the subject matter is that which was surrendered during the original prosecution. Finally, the reissue claims must be analyzed to determine whether they were materially narrowed in other respects.

7. The reissue claims are broader in scope than the patented claims since the Applicant has removed the limitation that the “second logical process [executing on the second electronic data processor is] capable of exchanging data across a network of one or more computers . . . .” The reissue application has been broadened to read on any multiprocessor system capable of exchanging data over a network instead of having a dedicated processor for communicating across a network. The claims have also been further broadened by the Applicant's removal of the limitation that the data from both processors are combined to be displayed in a windowed format on a display terminal.

Art Unit: 2439

8. The subject matter cancelled in the reissue application was surrendered during the course of the original prosecution. As noted by the cases cited and the amendments made by the Applicant, the Examiner interpreted the claims as having a processor dedicated to network communications and the claimed system to display the data from both processors in a windowed format. This interpretation was supported by the Applicant's final amendment prior to allowance, which further specified that the system comprised two processors, one of which was capable of exchanging data across a network, and combining and displaying the data from the processes executing on the separate processors. The reissue claims were not materially narrowed in other respects, and therefore recapture exists.

#### **Claim Rejections - 35 USC § 112**

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claim 25 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 25 recites the limitation "the portable wireless communication device" in the preamble. There is insufficient antecedent basis for this limitation in the claim.

11. Claims 44-57 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. A single claim which claims both an apparatus and the method steps of using the apparatus is indefinite under 35 U.S.C. 112, second paragraph. MPEP § 2173.05(p)(II). See also *IPXL Holdings v. Amazon.com, Inc.*, 430 F.2d 1377, 1384, 77 USPQ2d 1140, 1145 (Fed. Cir. 2005); *Ex parte Lyell*, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990). Claims 44-57 are



Art Unit: 2439

directed toward a portable computing device and a method of using it and are therefore indefinite under 35 U.S.C. 112, second paragraph.

### **Claim Rejections - 35 USC § 101**

12. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

13. Claims 44-57 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. A single claim which claims both an apparatus and the method steps of using the apparatus is neither a “process” nor a “machine,” but rather embraces or overlaps two different statutory classes of invention set forth in 35 U.S.C. 101 which is drafted so as to set forth the statutory classes of invention in the alternative only. MPEP § 2173.05(p)(II). See also *IPXL Holdings v. Amazon.com, Inc.*, 430 F.2d 1377, 1384, 77 USPQ2d 1140, 1145 (Fed. Cir. 2005); *Ex parte Lyell*, 17 USPQ2d 1548 (Bd. Pat. App. & Inter. 1990). Since the claims set forth a portable computing device and a method of using it, thereby overlapping two statutory classes of invention, they are ineligible for patent protection under 35 U.S.C. 101.

### **Claim Rejections - 35 USC § 102**

14. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2439

15. Claims 32-36, 39-48, and 51-57 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 7,146,305 B2 to van der Made, hereinafter van der Made.

16. As per claim 32, van der Made teaches a method of operating a portable computer having at least one electronic data processor communicatively coupled to a first and second memory space and to a network interface device, wherein the network interface device is configured to exchange data across a network of one or more computers using a wireless connection, comprising the steps of:

storing at least one system file within the first memory space (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6);

executing a first browser process in a first logical process using the at least one electronic data processor, wherein the first logical process is configured to access data contained in the first memory space (Figures 1 [element 105], 3 [element 105], column 1, lines 22-55, column 5, lines 24-55, i.e. the invention relates to programs used in communication networks, including e-mail and web browsing applications);

executing a second browser process in a second logical process using the at least one electronic data processor, wherein the second logical process is configured to access data contained in the second memory space and is further configured to generate video data (Figures 1 [elements 104, 205], 3 [elements 104, 205], column 6, lines 16-43, the processor generates video data for the I/O-GUI element 104);

opening the second browser process on instruction from the first browser process (column 5, line 50 to column 6, line 6, an application process initializing the analytic virtual machine);

Art Unit: 2439

passing data from the first browser process to the second browser process (column 5, line 50 to column 6, line 31);

displaying video data from the second browser process (column 5, lines 24-55, column 6, lines 38-43, the resulting behavior flag pattern, together with the sequencer structure, are passed to the application that initiated the analytical virtual machine which in turn displays the data on the I/O-GUI of element 104);

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process (column 9, lines 47-60, column 10, lines 29-44).

17. Regarding claim 33, van der Made teaches wherein the portable computer is configured such that the first browser process is capable of exchanging data with the network interface device and with the second browser process (column 1, lines 22-55, column 5, lines 24-55, column 5, lines 24-55, column 6, lines 38-43).

18. With regards to claim 34, van der Made teaches downloading data from the network and passing the data from the first browser process to the second browser process (column 1, lines 22-55, column 5, lines 24-55, column 5, lines 24-55, column 6, lines 38-43).

19. Regarding claim 35, van der Made teaches wherein the portable computer is configured such that the second browser process is capable of exchanging data with the network interface

Art Unit: 2439

device and with the first browser process (column 5, lines 24-55, column 6, lines 38-43, the resulting behavior flag pattern, together with the sequencer structure, are passed to the application that initiated the analytical virtual machine).

20. Regarding claim 36, van der Made teaches wherein the second memory space is selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6); a partition on a memory device (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6); random access memory (RAM); both volatile and nonvolatile memory.

21. Regarding claim 39, van der Made teaches deleting at least one corrupted data file residing on the second memory space when the second logical process is terminated (column 6, lines 6-42).

22. Regarding claim 40, van der Made teaches wherein the at least one electronic data processor is selected from the group consisting of: an Application Specific Integrated Circuit; a Field Programmable Gate Array; a plurality of electronic data processors (Figures 1 [elements 105, 205], 3 [elements 105, 205]); a multi-core electronic data processor.

23. Regarding claim 41, van der Made teaches wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process (column 9, lines 47-60, column 10, lines 29-44).

Art Unit: 2439

24. Regarding claim 42, van der Made teaches displaying video data from the first browser process (column 9, lines 47-60, column 10, lines 29-44).

25. Regarding claim 43, van der Made teaches wherein attempts by malware to record data entry by the computer user are effectively blocked (column 9, lines 47-60, column 10, lines 29-44).

26. As per claim 44, van der Made teaches a portable computer, comprising:

a network interface device configured to exchange data across a network of one or more computers using a wireless connection (column 1, lines 22-55, column 5, lines 24-55, i.e. the invention relates to programs used in communication networks, including wired and wireless connections);

at least a first memory space and a second memory space (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6);

at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, wherein the user interface is configured to receive input from a computer user (Figures 1 [element 105], 3 [element 105], column 1, lines 22-55, column 5, lines 24-55);

wherein the portable computer is configured for performing the steps of:

storing at least one system file in the first memory space (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6);

Art Unit: 2439

opening a first browser process, wherein the first browser process is capable of accessing data contained in the first memory space (Figures 1 [element 105], 3 [element 105], column 1, lines 22-55, column 5, lines 24-55, i.e. the invention relates to programs used in communication networks, including e-mail and web browsing applications);

opening a second browser process, wherein the second browser process is capable of accessing data contained in the second memory space, and is further capable of generating video data (Figures 1 [elements 104, 205], 3 [elements 104, 205], column 5, line 50 to column 6, line 6, column 6, lines 16-43, an application process initializing the analytic virtual machine, the analytical machine processor generates video data for the I/O-GUI element 104);

passing data from the first browser process to the second browser process (column 5, line 50 to column 6, line 31);

displaying video data from the second browser process (column 5, lines 24-55, column 6, lines 38-43, the resulting behavior flag pattern, together with the sequencer structure, are passed to the application that initiated the analytical virtual machine which in turn displays the data on the I/O-GUI of element 104);

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process (column 9, lines 47-60, column 10, lines 29-44).

27. Regarding claim 45, van der Made teaches wherein the first browser process is capable of exchanging data with the network interface device and with the second browser process (column

Art Unit: 2439

1, lines 22-55, column 5, lines 24-55, column 5, lines 24-55, column 6, lines 38-43).

28. With regards to claim 46, van der Made teaches performing the step of downloading data from the network and passing the downloaded data from the first browser process to the second browser process (column 1, lines 22-55, column 5, lines 24-55, column 5, lines 24-55, column 6, lines 38-43).

29. Concerning claim 47, van der Made teaches performing the step of storing the downloaded data on the second memory space (column 1, lines 22-55, column 5, lines 24-55, column 5, lines 24-55, column 6, lines 38-43).

30. Regarding claim 48, van der Made teaches wherein the second browser process is capable of exchanging data with the network interface device and with the first browser process (column 5, lines 24-55, column 6, lines 38-43, the resulting behavior flag pattern, together with the sequencer structure, are passed to the application that initiated the analytical virtual machine).

31. Regarding claim 51, van der Made teaches that at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated (column 6, lines 6-42).

32. Regarding claim 52, van der Made teaches wherein the first browser process is protected

Art Unit: 2439

from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process (column 9, lines 47-60, column 10, lines 29-44).

33. Regarding claim 53, van der Made teaches the first browser process instructing the second browser process to open (column 5, line 50 to column 6, line 31).

34. Regarding claim 54, van der Made teaches wherein attempts by malware to record data entry by the computer user are effectively blocked (column 9, lines 47-60, column 10, lines 29-44).

35. Regarding claim 55, van der Made teaches wherein the at least one electronic data processor is selected from the group consisting of: an Application Specific Integrated Circuit; a Field Programmable Gate Array; a plurality of electronic data processors (Figures 1 [elements 105, 205], 3 [elements 105, 205]); a multi-core electronic data processor.

36. Regarding claim 56, van der Made teaches wherein the second memory space is selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6); a partition on a memory device (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6); random access memory (RAM); both volatile and nonvolatile memory ( ).



Art Unit: 2439

37. Regarding claim 57, van der Made teaches the first browser process opening a plurality of second browser processes (column 5, line 50 to column 6, line 31).

**Claim Rejections - 35 USC § 103**

38. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

39. Claims 1-5, 7, 10, 11, and 14-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over van der Made in view of U.S. Patent No. 6,871,348 B1 to Cooper, hereinafter Cooper.

40. As per claim 1, van der Made teaches a method of operating a computer system capable of exchanging data across a network of one or more computers and having at least a first and second electronic data processor capable of executing instructions using a common operating system, comprising the steps of:

executing browser instructions in a first logical process within the common operating system using the first electronic data processor, wherein the first logical process is capable of accessing data contained in a first memory space (Figures 1 [element 105], 3 [element 105], column 1, lines 22-55, column 5, lines 24-55, i.e. the invention relates to programs used in communication networks, including e-mail and web browsing applications);

executing instructions in a second logical process within the common operating system using the second electronic data processor, wherein the second logical process is capable of

Art Unit: 2439

accessing data contained in the second memory space (Figures 1 [element 205], 3 [element 205], column 6, lines 16-43);

wherein the computer system is configured such that data residing on the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second logical process (column 9, lines 47-60, column 10, lines 29-44).

41. Van der Made discloses a user I/O and GUI (Figures 1 [element 104], 3 [element 104]) that displays application data being executed by both the processor and the software CPU (column 5, lines 24-55, column 6, lines 38-43, the resulting behavior flag pattern, together with the sequencer structure, are passed to the application that initiated the analytical virtual machine). However, van der Made does not explicitly disclose displaying data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to a display.

42. Cooper discloses displaying data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to a display (column 3, lines 1-51).

43. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the data from the first and second processes to be displayed together, since one of ordinary skill in the art would recognize that it would be more efficient to combine data instead of having the first processor execute code that was performed on the second processor. Furthermore, as Cooper states at column 2, lines 55-67, that the combined display would present

Art Unit: 2439

only one application to the user, thereby providing a cleaner, more aesthetically pleasing desktop that would be easier to maneuver.

44. Regarding claim 2, van der Made teaches wherein the second memory space is selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6); a partition on a memory device (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6); random access memory (RAM); both volatile and nonvolatile memory.

45. Regarding claim 3, van der Made teaches wherein the second logical process is selected from the group consisting of: an electronic mail process (column 1, lines 22-37), an instant messaging process, an internet browser process, an interactive gaming process, a virtual private network (VPN) process, and a reader application process.

46. Regarding claim 4, van der Made teaches wherein the first logical process receives user interface data and passes the user interface data to the second logical process (column 5, line 50 to column 6, line 43).

47. With regards to claim 5, van der Made teaches wherein the second memory space is selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6,

Art Unit: 2439

line 6); a partition on a memory device (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6); random access memory (RAM); both volatile and nonvolatile memory.

48. Regarding claim 7, van der Made teaches automatically deleting at least one data file residing on the second memory space when the second logical process is terminated (column 6, lines 16-43).

49. As per claims 10 and 15, van der Made teaches a multiprocessor computer system using a common operating system capable of exchanging data across a network of one or more computers via a network interface device, comprising the steps of:

a first electronic data processor capable of executing browser instructions using the common operating system and communicatively coupled to a first memory space (Figures 1 [element 105], 3 [element 105], column 1, lines 22-55, column 5, lines 24-55, i.e. the invention relates to programs used in communication networks, including e-mail and web browsing applications);

a second electronic data processor capable of executing browser instructions using the common operating system and communicatively coupled to a second memory space (Figures 1 [element 205], 3 [element 205], column 6, lines 16-43);

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first electronic memory space is protected from corruption by a malware process downloaded from the network and executing on the second electronic data processor (column 9, lines 47-60, column 10, lines 29-44).

Art Unit: 2439

50. Van der Made discloses a user I/O and GUI (Figures 1 [element 104], 3 [element 104]) that displays application data being executed by both the processor and the software CPU (column 5, lines 24-55, column 6, lines 38-43, the resulting behavior flag pattern, together with the sequencer structure, are passed to the application that initiated the analytical virtual machine). However, van der Made does not explicitly disclose a video processor adapted to combine video data from the first and second electronic data processors and transmit the combined video data to a display.

51. Cooper discloses displaying data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to a display (column 3, lines 1-51).

52. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the data from the first and second processes to be displayed together, since one of ordinary skill in the art would recognize that it would be more efficient to combine data instead of having the first processor execute code that was performed on the second processor. Furthermore, as Cooper states at column 2, lines 55-67, that the combined display would present only one application to the user, thereby providing a cleaner, more aesthetically pleasing desktop that would be easier to maneuver.

53. Regarding claim 11, van der Made teaches wherein the second memory space is selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6);

Art Unit: 2439

a partition on a memory device (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6); random access memory (RAM); both volatile and nonvolatile memory.

54. Regarding claims 14 and 16, van der Made teaches wherein the computer system is configured such that a malware program downloaded from the network and executing on the second electronic data processor is incapable of initiating the execution of instructions on the first electronic data processor (column 10, lines 42-45, no direct interaction between the two processors).

55. Regarding claim 17, van der Made teaches at least one network interface device capable of exchanging data with the network and with a logical process selected from the group consisting of: the first logical process, the second logical process (column 1, lines 22-55, column 5, lines 24-55, i.e. the invention relates to programs used in communication networks, including e-mail and web browsing applications).

56. Claims 6 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over van der Made in view of Cooper as applied above, and further in view of U.S. Patent No. 7,024,581 B1 to Wang et al., hereinafter Wang.

57. Regarding claims 6 and 20, van der Made and Cooper do not teach restoring at least one corrupted data file from a protected image.

Art Unit: 2439

58. Wang teaches restoring at least one corrupted data file from a protected image (Figures 2 [elements 82, 72, 74, 76, 78, 80], 3 [element 140], 6 [element 236], 7 [element 272], column 9, lines 13-30, column 9, line 31-67).

59. It would have been obvious to one of ordinary skill in the art at the time the invention was made to restore at least one corrupted data file from a protected image, since Wang states at column 2, lines 49-60 that using a protected image takes advantage of today's computing power and storage capabilities to increase the reliability, accessibility, flexibility, and performance of computers and the backup/restore process.

60. Claims 12 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over van der Made in view of Cooper as applied above, and further in view of U.S. Patent No. 6,578,140 B1 to Policard, hereinafter Policard.

61. Regarding claim 12, van der Made and Cooper do not teach wherein the first and second electronic data processors are part of a dual processor computer system.

62. Policard teaches wherein the first and second electronic data processors are part of a dual processor computer system (Figure 4 [elements 34, 52], column 4, lines 11-21).

63. It would have been obvious to one of ordinary skill in the art to replace the virtual processor of van der Made with a dedicated processor, since one of ordinary skill in the art would recognize and appreciate the performance enhancement accompanied by having a dedicated hardware processor to perform suspect operations over the software processor described in van der Made.

Art Unit: 2439

64. Regarding claim 19, van der Made and Cooper do not teach wherein the at least one electronic data processor is selected from the group consisting of: a multi-core electronic data processor; dual electronic data processors.

65. Policard teaches wherein the at least one electronic data processor is selected from the group consisting of: a multi-core electronic data processor; dual electronic data processors (Figure 4 [elements 34, 52], column 4, lines 11-21).

66. It would have been obvious to one of ordinary skill in the art to replace the virtual processor of van der Made with a dedicated processor, since one of ordinary skill in the art would recognize and appreciate the performance enhancement accompanied by having a dedicated hardware processor to perform suspect operations over the software processor described in van der Made.

67. Claims 21-26 and 29-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over van der Made.

68. As per claim 21, van der Made teaches a portable computer, comprising:

a network interface device configured to exchange data across a network of one or more computers using a wireless connection (column 1, lines 22-55, column 5, lines 24-55, i.e. the invention relates to programs used in communication networks, including wired and wireless connections);

at least a first memory space and a second memory space, the first memory space containing at least one system file (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6);



Art Unit: 2439

at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, wherein the user interface is configured to receive input from a computer user (Figures 1 [element 105], 3 [element 105], column 1, lines 22-55, column 5, lines 24-55);

the at least one electronic data processor configured to execute a first browser process in a first logical process, wherein the first logical process is capable of accessing data contained in the first memory space (Figures 1 [element 105], 3 [element 105], column 1, lines 22-55, column 5, lines 24-55, i.e. the invention relates to programs used in communication networks, including e-mail and web browsing applications);

the at least one electronic data processor further configured to execute a second browser process in a second logical process, wherein the second logical process is capable of accessing data contained in the second memory space and is further capable of generating video data (Figures 1 [elements 104, 205], 3 [elements 104, 205], column 6, lines 16-43, the processor generates video data for the I/O-GUI element 104);

a virtual processor configured to transmit video data from the second browser process to a display (column 5, lines 24-55, column 6, lines 38-43, the resulting behavior flag pattern, together with the sequencer structure, are passed to the application that initiated the analytical virtual machine which in turn displays the data on the I/O-GUI of element 104);

wherein the first browser process is capable of opening the second browser process and is further capable of passing data to the second browser process (column 5, line 45 to column 6, line 6);

Art Unit: 2439

wherein further the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing within the second browser process (column 9, lines 47-60, column 10, lines 29-44).

69. Van der Made does not teach a video processor configured to transmit video data from the second browser process to a display.

70. It would have been obvious to one of ordinary skill in the art at the time invention was made to replace the virtual processor of van der Made with a hardware video processor, since one of ordinary skill would recognize the benefits in speed, performance, and efficiency in replacing a virtual processor with an actual hardware processor.

71. Regarding claim 22, van der Made teaches wherein the first browser process is capable of exchanging data with the network interface device and with the second browser process (column 1, lines 22-55, column 5, lines 24-55, column 5, lines 24-55, column 6, lines 38-43).

72. With regards to claim 23, van der Made teaches wherein the first browser process is capable of passing data downloaded from the network to the second browser process (column 1, lines 22-55, column 5, lines 24-55, column 5, lines 24-55, column 6, lines 38-43).

73. Regarding claim 24, van der Made teaches wherein the second browser process is capable of exchanging data with the network interface device and with the first browser process (column 5, lines 24-55, column 6, lines 38-43, the resulting behavior flag pattern, together with the

Art Unit: 2439

sequencer structure, are passed to the application that initiated the analytical virtual machine).

74. Regarding claim 25, van der Made teaches wherein the at least one electronic data processor is selected from the group consisting of: an Application Specific Integrated Circuit; a Field Programmable Gate Array; a plurality of electronic data processors (Figures 1 [elements 105, 205], 3 [elements 105, 205]); a multi-core electronic data processor.

75. Regarding claim 26, van der Made teaches wherein the second memory space is selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6); a partition on a memory device (Figures 1 [element 106], 3 [element 106], column 5, line 55 to column 6, line 6); random access memory (RAM); both volatile and nonvolatile memory.

76. Regarding claim 29, van der Made teaches at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated (column 6, lines 6-42).

77. Regarding claim 30, van der Made teaches that the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process (column 9, lines 47-60, column 10, lines 29-44).

78. Regarding claim 31, van der Made teaches wherein attempts by malware to record data

Art Unit: 2439

entry by the computer user are effectively blocked (column 9, lines 47-60, column 10, lines 29-44).

79. Claims 27, 28, 37, 38, 49, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over van der Made in view of Wang.

80. Regarding claims 27, 37, and 49, van der Made does not teach at least one corrupted file required for a browser process is capable of being restored from a protected image.

81. Wang teaches at least one corrupted file required for a browser process is capable of being restored from a protected image (Figures 2 [elements 82, 72, 74, 76, 78, 80], 3 [element 140], 6 [element 236], 7 [element 272], column 9, lines 13-30, column 9, line 31-67).

82. It would have been obvious to one of ordinary skill in the art at the time the invention was made to restore at least one corrupted data file from a protected image, since Wang states at column 2, lines 49-60 that using a protected image takes advantage of today's computing power and storage capabilities to increase the reliability, accessibility, flexibility, and performance of computers and the backup/restore process.

83. With regards to claims 28, 38, and 50, Wang teaches wherein the protected image is stored at a location selected from the group consisting of: a removable drive; the first memory space; a partition on a memory device (Figures 2 [elements 82, 72, 74, 76, 78, 80], 3 [element 140], 6 [element 236], 7 [element 272], 9 [element 309], column 9, lines 13-30, column 9, line 31-67); a nonvolatile memory disk; another device (Figure 4).

Art Unit: 2439

### **Allowable Subject Matter**

84. Claims 8, 9, 13, and 18 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Claims 8, 9, 13, and 18 would be allowable if the rejections set forth in this Office action were overcome and all of the limitations of the base claim and any intervening claims were included in those claims.

### **Conclusion**

85. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

86. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

87. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/

Application/Control Number: 12/720,147

Page 26

Art Unit: 2439

Primary Examiner, Art Unit 2439

clf

<b>Notice of References Cited</b>	Application/Control No. 12/720,147	Applicant(s)/Patent Under Reexamination ROZMAN ET AL.	
	Examiner Christian LaForgia	Art Unit 2439	Page 1 of 3

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification	
*	A	US-5,564,051 A	10-1996	Halliwell et al.	1/1
*	B	US-5,673,403 A	09-1997	Brown et al.	715/744
*	C	US-5,751,979 A	05-1998	McCrary, Duane J.	715/803
*	D	US-5,974,549 A	10-1999	Golan, Gilad	726/23
*	E	US-6,192,477 B1	02-2001	Corthell, David	726/11
*	F	US-6,199,181 B1	03-2001	Rechef et al.	714/38
*	G	US-6,385,721 B1	05-2002	Puckette, Robert B. E.	713/2
*	H	US-6,578,140 B1	06-2003	Policard, Claude M	713/1
*	I	US-2003/0221114 A1	11-2003	Hino et al.	713/189
*	J	US-6,678,712 B1	01-2004	McLaren et al.	718/100
*	K	US-2004/0039944 A1	02-2004	Karasaki, Teiji	713/201
*	L	US-6,754,815 B1	06-2004	Ellison et al.	713/1
*	M	US-2005/0005153 A1	01-2005	Das et al.	713/200

**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

**NON-PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<b>Notice of References Cited</b>	Application/Control No. 12/720,147	Applicant(s)/Patent Under Reexamination ROZMAN ET AL.	
	Examiner Christian LaForgia	Art Unit 2439	Page 2 of 3

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification	
*	A	US-6,871,348 B1	03-2005	Cooper, Frederick J.	719/310
*	B	US-2005/0198692 A1	09-2005	Zurko et al.	726/024
*	C	US-6,996,828 B1	02-2006	Kimura et al.	719/319
*	D	US-7,013,484 B1	03-2006	Ellison et al.	726/26
*	E	US-7,024,555 B2	04-2006	Kozuch et al.	726/22
*	F	US-7,024,581 B1	04-2006	Wang et al.	714/2
*	G	US-7,082,615 B1	07-2006	Ellison et al.	726/26
*	H	US-7,146,305 B2	12-2006	van der Made, Peter A. J.	703/22
*	I	US-7,146,640 B2	12-2006	Goodman et al.	726/16
*	J	US-7,260,839 B2	08-2007	Karasaki, Teiji	726/11
*	K	US-7,367,057 B2	04-2008	Das et al.	726/24
*	L	US-7,484,247 B2	01-2009	Rozman et al.	726/34
*	M	US-7,657,419 B2	02-2010	van der Made, Peter A. J.	703/22

**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

**NON-PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)			
	U				
	V				
	W				
	X				

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



<b>Notice of References Cited</b>	Application/Control No. 12/720,147	Applicant(s)/Patent Under Reexamination ROZMAN ET AL.	
	Examiner Christian LaForgia	Art Unit 2439	Page 3 of 3

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-7,818,808 B1	10-2010	Neiger et al.	726/26
*	B US-7,849,310 B2	12-2010	Watt et al.	713/164
*	C US-7,854,008 B1	12-2010	Huang et al.	726/24
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			

**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

**NON-PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	U				
	V				
	W				
	X				

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<b>Index of Claims</b>  <b>*1272014</b>  <b>7*</b>	<b>Application/Control No.</b> 12720147	<b>Applicant(s)/Patent Under Reexamination</b> ROZMAN ET AL.
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE									
Final	Original	12/29/2010									
	1	✓									
	2	✓									
	3	✓									
	4	✓									
	5	✓									
	6	✓									
	7	✓									
	8	✓									
	9	✓									
	10	✓									
	11	✓									
	12	✓									
	13	✓									
	14	✓									
	15	✓									
	16	✓									
	17	✓									
	18	✓									
	19	✓									
	20	✓									
	21	✓									
	22	✓									
	23	✓									
	24	✓									
	25	✓									
	26	✓									
	27	✓									
	28	✓									
	29	✓									
	30	✓									
	31	✓									
	32	✓									
	33	✓									

<b>Index of Claims</b>  <b>*1272014</b>  <b>7*</b>	<b>Application/Control No.</b> 12720147	<b>Applicant(s)/Patent Under Reexamination</b> ROZMAN ET AL.
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>

<b>N</b>	<b>Non-Elected</b>
<b>I</b>	<b>Interference</b>

<b>A</b>	<b>Appeal</b>
<b>O</b>	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/29/2010							
	34	✓							
	35	✓							
	36	✓							
	37	✓							
	38	✓							
	39	✓							
	40	✓							
	41	✓							
	42	✓							
	43	✓							
	44	✓							
	45	✓							
	46	✓							
	47	✓							
	48	✓							
	49	✓							
	50	✓							
	51	✓							
	52	✓							
	53	✓							
	54	✓							
	55	✓							
	56	✓							
	57	✓							

<b>Search Notes</b>  <b>*1272014</b>  <b>7*</b>	<b>Application/Control No.</b>  12720147	<b>Applicant(s)/Patent Under Reexamination</b>  ROZMAN ET AL.
	<b>Examiner</b>  Christian LaForgia	<b>Art Unit</b>  2439

<b>SEARCHED</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>
none	none	12/29/10	clf

<b>SEARCH NOTES</b>		
<b>Search Notes</b>	<b>Date</b>	<b>Examiner</b>
updated search for 10/913,609 (USPN 7,484,247)	12/29/10	clf

<b>INTERFERENCE SEARCH</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>

	/Christian LaForgia/ Primary Examiner.Art Unit 2439
--	--



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 8473

<b>SERIAL NUMBER</b> 12/720,147	<b>FILING or 371(c) DATE</b> 03/09/2010 <b>RULE</b>	<b>CLASS</b> 726	<b>GROUP ART UNIT</b> 2439	<b>ATTORNEY DOCKET NO.</b> ARAC-01RE1	
<b>APPLICANTS</b> Allen F. Rozman, Garland, TX; Alfonso J. Cioffi, Murphy, TX; <b>** CONTINUING DATA *****</b> This application is a REI of 10/913,609 08/07/2004 PAT 7,484,247 <b>** FOREIGN APPLICATIONS *****</b> <b>** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY **</b> 03/11/2010					
Foreign Priority claimed <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No 35 USC 119(a-d) conditions met <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Verified and /CHRISTIAN A LAFORGIA/ Acknowledged Examiner's Signature	<input type="checkbox"/> Met after Allowance Initials	<b>STATE OR COUNTRY</b> TX	<b>SHEETS DRAWINGS</b> 10	<b>TOTAL CLAIMS</b> 57	<b>INDEPENDENT CLAIMS</b> 6
<b>ADDRESS</b> Allen F. Rozman 6402 Wildlife Trail Garland, TX 75044					
<b>TITLE</b> SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE					
<b>FILING FEE RECEIVED</b> 2052	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:		<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit		

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number		12720147
	Filing Date		2010-03-09
	First Named Inventor	Rozman et al.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		ARAC-01RE1

U.S.PATENTS						<a href="#">Remove</a>
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/CLF/	1	5673403	B2	1997-09-30	Brown, et al	
/CLF/	2	5751979	B2	1998-05-12	McCrory	
/CLF/	3	5974549	B2	1999-10-26	Golan	
/CLF/	4	5978917	B2	1999-11-02	Chi	
/CLF/	5	6091412	B2	2000-07-18	Simonoff, et al	
/CLF/	6	6134661	B2	2000-10-17	Topp	
/CLF/	7	6397242	B1	2002-05-28	Devine, et al	
/CLF/	8	6401134	B1	2002-06-04	Razavi, et al	

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number	12720147
Filing Date	2010-03-09
First Named Inventor	Rozman et al.
Art Unit	
Examiner Name	
Attorney Docket Number	ARAC-01RE1

/CLF/	9	6433794	B1	2002-08-09	Beadle, et al	
/CLF/	10	6438600	B1	2002-08-20	Greenfield, et al	
/CLF/	11	6492995	B1	2002-12-10	Atkin, et al	
/CLF/	12	6678825	B1	2004-01-13	Ellison, et al	
/CLF/	13	6691230	B1	2004-02-10	Bardon	
/CLF/	14	6757685	B1	2004-06-29	Rafaelle, et al	
/CLF/	15	6836885	B1	2004-12-28	Buswell, et al	
/CLF/	16	7024555	B1	2006-04-06	Kozuch, et al	
/CLF/	17	7139890	B1	2006-11-21	Moran, et al	
/CLF/	18	7146640	B1	2006-12-05	Goodman, et al	
/CLF/	19	7260839	B1	2007-08-21	Karasaki	

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number	12720147
Filing Date	2010-03-09
First Named Inventor	Rozman et al.
Art Unit	
Examiner Name	
Attorney Docket Number	ARAC-01RE1

/CLF/	20	7401230	B1	2008-08-15	Campbell, et al	
/CLF/	21	7421689	B1	2008-09-02	Ross, et al	
/CLF/	22	7565522	B1	2009-07-21	Sastry, et al	

If you wish to add additional U.S. Patent citation information please click the Add button.

**U.S.PATENT APPLICATION PUBLICATIONS**

Examiner Initial*	Cite No	Publication Number	Kind Code <sup>1</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

**FOREIGN PATENT DOCUMENTS**

Examiner Initial*	Cite No	Foreign Document Number <sup>3</sup>	Country Code <sup>2</sup>	Kind Code <sup>4</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T <sup>5</sup>
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button

**NON-PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>5</sup>
/CLF/	1	Architecture of Virtual Machines by R. P. GOLDBERG, Honeywell Information Systems, Inc. and Harvard University presented at the AFIPS National Computer Conference, New York, New York, June 4-8, 1973.	<input type="checkbox"/>



**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		12720147
Filing Date		2010-03-09
First Named Inventor	Rozman et al.	
Art Unit		
Examiner Name		
Attorney Docket Number		ARAC-01RE1

/CLF/	2	The Duality of Memory and Communication in the Implementation of a Multiprocessor Operating System by MICHAEL YOUNG, AVADIS TEVANIAN, RICHARD RASHEED, DAVID GOLUB, JEFFERY EPPINGER, JONATHAN CREW, WILLIAM BOLOSKY, DAVID BLACK and ROBERT BARON, Computer Science Department Carnegie-Mellon University Appeared in Proceedings of the 11th Operating Systems Principles, November, 1987	<input type="checkbox"/>
/CLF/	3	Application-Controlled Physical Memory using External Page-Cache Management by KEIRAN HARTY and DAVID R. CHERITON, Computer Science Department, Stanford University, 1992	<input type="checkbox"/>
/CLF/	4	Efficient Software-Based Fault Isolation by ROBERT WAHBE, STEVEN LUCCO, THOMAS ANDERSON, SUSAN GRAHAM, Computer Science Division University of California, Berkeley, SIGOPS 1993	<input type="checkbox"/>
/CLF/	5	TRON: Process-Specific File Protection for the UNIX Operating System by ANDREW BERMAN, VIRGIL BOURASSA, ERIK SELBERG, Department of Computer Science and Engineering, University of Washington, January 23, 1995	<input type="checkbox"/>
/CLF/	6	A Secure Environment for Untrusted Helper Applications (Confining the Wily Hacker) by IAN GOLDBERG, DAVID WAGNER, RANDI THOMAS, and ERIC BREWER, Computer Science Division, University of California, Berkeley, Sixth USENIX UNIX Security Symposium San Jose, California, July 1996	<input type="checkbox"/>
/CLF/	7	Building Systems that Flexibly Control Downloaded Executable Context by TRENT JAEGER and ATUL PRAKASH, Software Systems Research Lab, University of Michigan and AVIEL D. RUBIN, Security Research Group, Bellcore Sixth USENIX UNIX Security Symposium San Jose, California, July 1996	<input type="checkbox"/>
/CLF/	8	Java Security: From HotJava to Netscape and Beyond by DREW DEAN, EDWARD W. FELTEN, DAN S. WALLACH Department of Computer Science, Princeton University, Princeton, NJ 08544 1996 IEEE Symposium on Security and Privacy, Oakland, CA, May 6-8, 1996.	<input type="checkbox"/>
/CLF/	9	ChakraVyuha (CV) : A Sandbox Operating System Environment for Controlled Execution of Alien Code by ASIT DAN, AJAY MOHINDRA, RAJIV RAMASWAMI, and DINKAR SITARAM IBM Research Division T.J. Watson Research Center Yorktown Heights, New York RC 20742 (2/20/97) Computer Science IBM Research Report LIMITED DISTRIBUTION	<input type="checkbox"/>
/CLF/	10	Vulnerability of Secure Web Browsers by FLAVIO DE PAOLI, ANDRE DOS SANTOS, RICHARD KEMMERER Reliable Software Group Computer Science Department, University of California, Santa Barbara, 1997	<input type="checkbox"/>
/CLF/	11	Security of Web Browser Scripting Languages: Vulnerabilities, Attacks, and Remedies by VINOD ANUPAM and ALAIN MAYER, Bell Laboratories, Lucent Technologies 7th USENIX Security Symposium San Antonio, Texas, January 26-29, 1998	<input type="checkbox"/>
/CLF/	12	"Virtual Memory in Contemporary Microprocessors" by BRUCE JACOB University of Maryland and TREVOR MUDGE University of Michigan, IEEE MICRO JULY-AUGUST 1998	<input type="checkbox"/>

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		12720147
Filing Date		2010-03-09
First Named Inventor	Rozman et al.	
Art Unit		
Examiner Name		
Attorney Docket Number		ARAC-01RE1

/CLF/	13	"Flexible Control of Downloaded Executable Content" by TRENT JAEGER and JOCHEN LIEDTKE and NAYEEM ISLAM, IBM Thomas J. Watson Research Center, and ATUL PRAKASH University of Michigan, Ann Arbor ACM Transactions on Information and System Security, Vol. 2, No. 2, May 1999, Pages 177–228.	<input type="checkbox"/>
/CLF/	14	"J2ME Building Blocks for Mobile Devices: White Paper on KVM and the Connected", Limited Device Configuration Sun Microsystems May 19, 2000	<input type="checkbox"/>
/CLF/	15	"User-level Resource-constrained Sandboxing" by FANGZHE CHANG, AYAL ITZKOVITZ, and VIJAY KARAMCHETI Department of Computer Science, Courant Institute of Mathematical Sciences, New York University USENIX Windows System Symposium, August 2000	<input type="checkbox"/>
/CLF/	16	"Verifying the EROS Confinement Mechanism" by JONATHAN S. SHAPIRO and SAN WEBER IBM T.J. Watson Research Center 0-7695-0665-8/00 2000 IEEE	<input type="checkbox"/>
/CLF/	17	"WindowBox: A Simple Security Model for the Connected Desktop" by DIRK BALFANZ, Princeton University and DANIEL R. SIMON, Microsoft Research, 2000	<input type="checkbox"/>
/CLF/	18	"Building a Secure Web Browser" by SOTIRIS IOANNIDIS, University of Pennsylvania, and STEVEN M. BELLOVIN, AT&T Labs Research 2001 USENIX Annual Technical Conference Boston, Massachusetts, USA June 25–30, 2001	<input type="checkbox"/>
/CLF/	19	"Virtualizing I/O Devices on VMware Workstation's Hosted Virtual Machine Monitor" by JEREMY SUGERMAN, GANESH VENKITACHALAM and BENG-HONG LIM, VMware, Inc. 3145 Porter Dr, Palo Alto, CA 943042001 USENIX Annual Technical Conference Boston, Massachusetts, USA June 25–30, 2001	<input type="checkbox"/>
/CLF/	20	"When Virtual Is Better Than Real" by PETER M. CHEN and BRIAN D. NOBLE, Department of Electrical Engineering and Computer Science University of Michigan 2001	<input type="checkbox"/>
/CLF/	21	"A Flexible Containment Mechanism for Executing Untrusted Code" by DAVID PETERSON, MATT BISHOP, and RAJU PANDEY, Department of Computer Science University of California, Davis USENIX Security Symposium San Francisco, California, USA August 5-9, 2002	<input type="checkbox"/>
	22		<input type="checkbox"/>
/CLF/	23	"ReVirt: Enabling Intrusion Analysis through Virtual-Machine Logging and Replay" by GEORGE W. DUNLAP, SAMUEL T. KING, SUKRU CINAR, MURTAZA A. BASRAI, PETER M. CHEN, Department of Electrical Engineering and Computer Science, University of Michigan Proceedings of the 2002 Symposium on Operating Systems Design and Implementation (OSDI)	<input type="checkbox"/>

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		12720147
Filing Date		2010-03-09
First Named Inventor	Rozman et al.	
Art Unit		
Examiner Name		
Attorney Docket Number		ARAC-01RE1

/CLF/	24	"Trusted Paths for Browsers: An Open-Source Solution to Web Spoofing" by ZISHUANG (Eileen) YE and SEAN SMITH Department of Computer Science Dartmouth College Technical Report TR2002-418 February 4, 2002	<input type="checkbox"/>
/CLF/	25	"User Interaction Design for Secure Systems" by KA-PING YEE <a href="http://zesty.ca/sid/">http://zesty.ca/sid/</a> 2002	<input type="checkbox"/>
/CLF/	26	BAA-00-06-SNK Focused Research Topic 5 by MARC STIEGLER AND MARK MILLER Report Name: "A Capability Based Client: The DarpaBrowser" 26 June 2002	<input type="checkbox"/>
/CLF/	27	"A Virtual Machine Introspection Based Architecture for Intrusion Detection" by TAL GARFINKEL and MENDEL ROSENBLUM, Computer Science Department, Stanford University 2003	<input type="checkbox"/>
/CLF/	28	"Terra: A Virtual Machine-Based Platform for Trusted Computing" by TAL GARFINKEL, BEN PFAFF, JIM CHOW, DAN BONEH and MENDEL ROSENBLUM, Computer Science Department, Stanford University SOSP'03, October 19-22, 2003, Bolton Landing, New York, USA.	<input type="checkbox"/>
/CLF/	29	Microsoft® Virtual PC 2004 Technical Overview by JERRY HONEYCUTT Published November 2003 <a href="http://download.microsoft.com/download/c/f/b/cfb100a7-463d-4b86-ad62-064397178b4f/Virtual_PC_Technical_Overview.doc">http://download.microsoft.com/download/c/f/b/cfb100a7-463d-4b86-ad62-064397178b4f/Virtual_PC_Technical_Overview.doc</a>	<input type="checkbox"/>
/CLF/	30	"Xen and the Art of Virtualization" by PAUL BARHAM, BORIS DRAGOVIC, KEIR FRASER, STEVEN HAND, TIM HARRIS, ALEX HO, ROLF NEUGEBAUREY, IAN PRATT, ANDREW WARFIELD University of Cambridge Computer Laboratory 15 JJ Thomson Avenue, Cambridge, UK, CB3 0FD SOSP'03, October 19-22, 2003, Bolton Landing, New York, USA	<input type="checkbox"/>
/CLF/	31	"Design of the EROS Trusted Window System" by JONATHAN S. SHAPIRO, JOHN VANDERBURGH, ERIC NORTHROP, Systems Research Laboratory Johns Hopkins University, and, DAVID CHIZMADIA, Promia, Inc. 2004	<input type="checkbox"/>
/CLF/	32	"Survey of System Virtualization" Techniques by ROBERT ROSE March 8, 2004	<input type="checkbox"/>
/CLF/	33	White Paper: "Smart Phone Security Issues" by LUC DELPHA and MALIHA RASHEED, Cyber Risk Consulting Blackhat Briefings Europe May 2004	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number	12720147
Filing Date	2010-03-09
First Named Inventor	Rozman et al.
Art Unit	
Examiner Name	
Attorney Docket Number	ARAC-01RE1

**EXAMINER SIGNATURE**

Examiner Signature	/Christian LaForgia/	Date Considered	12/21/2010
--------------------	----------------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> See Kind Codes of USPTO Patent Documents at [www.USPTO.GOV](http://www.USPTO.GOV) or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>3</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>4</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here if English language translation is attached.

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	36	rozman-all\$.in.	US-PGPUB; USPAT	OR	OFF	2007/09/13 09:28
S2	2	cioffi-alf\$.in.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:49
S3	1	"6289462".pn.	US-PGPUB; USPAT	OR	OFF	2007/09/13 09:32
S4	10	((("7146640") or ("5835695") or ("6578140") or ("20050149933") or ("6892261") or ("6678712") or ("6957286") or ("6996828") or ("20040205755") or ("6697972")).PN.	US-PGPUB; USPAT	OR	OFF	2007/09/13 09:33
S5	5	("6578140").URPN.	USPAT	OR	OFF	2007/09/13 10:01
S6	1	(dual multiple) near (OS operat\$3 near systems) with (prevent\$3 stop\$4) with (virus trojan malicious malware)	US-PGPUB; USPAT	OR	ON	2007/09/13 10:06
S7	15	("6385721").URPN.	USPAT	OR	OFF	2007/09/13 10:03
S8	8	(dual multiple) near (OS operat\$3 near systems) with (virus trojan malicious malware)	US-PGPUB; USPAT	OR	ON	2007/09/13 13:58
S9	0	("2004/0039944").URPN.	USPAT	OR	OFF	2007/09/13 10:09

S10	35	(("5826013") or ("5978917") or ("6735700") or ("6663000") or ("6553377") or ("6216112") or ("4890098") or ("5555364") or ("5666030") or ("5995103") or ("5502808") or ("5280579") or ("5918039") or ("6480198") or ("6167522") or ("6199181") or ("6275938") or ("6351816") or ("6456554") or ("6658573") or ("6507904") or ("6633963") or ("6678825") or ("5751979") or ("20040054588") or ("20040034794") or ("20040006715") or ("20030177397") or ("20030097591") or ("20030023857") or ("20020066016") or ("20020174349") or ("6581162") or ("6134661") or ("6578140")).PN.	US-PGPUB; USPAT	OR	OFF	2007/09/13 10:13
S11	8	(US-20040039944-\$).did. or (US-7146640-\$ or US-6996828-\$ or US-6678712-\$ or US-6578140-\$ or US-6385721-\$ or US-7260839-\$ or US-6199181-\$).did.	US-PGPUB; USPAT	OR	OFF	2007/09/13 10:28
S12	0	S11 and network\$3 near (OS operat\$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 10:29
S13	8565	network\$3 near (OS operat\$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 10:29
S14	2	(dual multiple) near (OS operat\$3 near systems) same (display\$3) with both with (OS\$2 operat\$3 near systems)	US-PGPUB; USPAT	OR	ON	2007/09/13 11:55

S15	67	(dual multiple) near (OS operat\$3 near systems) same (display\$3) with (multiple) with (OS\$2 operat\$3 near systems)	US-PGPUB; USPAT	OR	ON	2007/09/13 11:55
S16	41	("5673403").URPN.	USPAT	OR	OFF	2007/09/13 12:12
S17	4565	(dual multiple) near (OS operat\$3 near systems)	US-PGPUB; USPAT	OR	ON	2007/09/13 14:49
S18	688	multi\$score near (processor cpu)	US-PGPUB; USPAT	OR	ON	2007/09/13 13:59
S19	37	S17 and S18	US-PGPUB; USPAT	OR	ON	2007/09/13 13:59
S20	18	S17 same S18	US-PGPUB; USPAT	OR	ON	2007/09/13 14:00
S21	4	S17 with S18	US-PGPUB; USPAT	OR	ON	2007/09/13 13:59
S22	14	S17 same S18 not S21	US-PGPUB; USPAT	OR	ON	2007/09/13 14:01
S23	19	S19 not S20	US-PGPUB; USPAT	OR	ON	2007/09/13 14:01
S24	665	(dual multiple) near (OS operat\$3 near systems) and (remov\$3 delet\$3) with (file program)	US-PGPUB; USPAT	OR	ON	2007/09/13 14:50
S25	1	(dual multiple) near (OS operat\$3 near systems) and (remov\$3 delet\$3) with (file program) with after near (run\$3 ran execut\$3)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:09
S26	17	(dual multiple) near (OS operat\$3 near systems) with encrypt\$3 \	US-PGPUB; USPAT	OR	ON	2007/09/13 15:09
S27	17	(dual multiple) near (OS operat\$3 near systems) with encrypt\$3	US-PGPUB; USPAT	OR	ON	2007/09/13 15:19
S28	36	(dual multiple) near (OS operat\$3 near systems) same encrypt\$3	US-PGPUB; USPAT	OR	ON	2007/09/13 15:19
S29	19	(dual multiple) near (OS operat\$3 near systems) same encrypt\$3 not S27	US-PGPUB; USPAT	OR	ON	2007/09/13 15:23
S30	676	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 not S28	US-PGPUB; USPAT	OR	ON	2007/09/13 15:33

S31	12	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (inter \$OS inter\$operat\$3 near system inter\$process\$2)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:35
S32	0	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (data information) with first near (OS operat\$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:38
S33	1	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with first near (OS operat\$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:37
S34	9	(US-20040039944-\$).did. or (US-7146640-\$ or US-6996828-\$ or US-6678712-\$ or US-6578140-\$ or US-6385721-\$ or US-7260839-\$ or US-6199181-\$ or US-5673403-\$).did.	US-PGPUB; USPAT	OR	OFF	2007/09/13 15:37
S35	2	S34 and encrypt\$3	US-PGPUB; USPAT	OR	ON	2007/09/13 15:37
S36	81	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (OS operat\$3 near system) with (transfer communicat \$3 data)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:39
S37	6	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (OS operat\$3 near system) with (transfer communicat \$3)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:39
S38	0	731/1.ccls.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:12
S39	2670	713/1.ccls.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:12
S40	1	"7027872".pn.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:52
S41	0	"7027872".pn. and IMD with (authentivat\$3 authori \$6 verif\$7 valid\$5)	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:52
S42	1	"7027872".pn. and (authentivat\$3 authori\$6 verif\$7 valid\$5)	US-PGPUB; USPAT	OR	OFF	2007/09/13 17:06



S43	1	"20050022020".pn.	US-PGPUB; USPAT	OR	OFF	2007/09/13 17:06
S44	1	"6192477".pn.	US-PGPUB; USPAT	OR	OFF	2008/02/19 13:13
S45	9	("6192477").URPN.	USPAT	OR	OFF	2008/02/19 13:14
S46	9	("6192477").URPN.	USPAT	OR	OFF	2008/06/16 16:15
S47	9	("6192477").URPN.	USPAT	OR	OFF	2008/06/16 16:15
S48	5	("6578140").URPN.	USPAT	OR	OFF	2008/08/18 14:31
S49	63	secure near3 process\$3 same insecure near3 process\$3	US-PGPUB; USPAT	OR	ON	2008/08/18 14:32
S50	1	secure near3 process\$3 same insecure near3 process\$3 with (internet e \$1mail)	US-PGPUB; USPAT	OR	ON	2008/08/18 14:32
S51	0	secure near3 processor and insecure near3 processor with (internet e \$1mail)	US-PGPUB; USPAT	OR	ON	2008/08/18 14:33
S52	9	("6192477").URPN.	USPAT	OR	OFF	2008/08/18 16:04
S53	1	common near (operat\$3 nears system OS) same protect\$3 near processor	US-PGPUB; USPAT	OR	ON	2008/08/18 16:33
S54	36	common near (operat\$3 nears system OS) and protect\$3 near processor	US-PGPUB; USPAT	OR	ON	2008/08/18 16:33
S55	0	(common near (operat\$3 nears system OS) and protect\$3 near processor). clm.	US-PGPUB; USPAT	OR	ON	2008/08/18 16:34
S56	1	"7484247".pn.	US-PGPUB; USPAT	OR	OFF	2010/12/21 13:22
S57	8	(("5673403") or ("5751979") or ("5974549") or ("5978917") or ("6091412") or ("6134661") or ("6397242") or ("6401134")).PN.	USPAT	OR	OFF	2010/12/21 13:27
S58	173	("5974549").URPN.	USPAT	OR	OFF	2010/12/21 13:29

S59	11	(("6433794") or ("6438600") or ("6492995") or ("6678825") or ("6691230") or ("6757685") or ("6836885") or ("7024555") or ("7139890") or ("7146640") or ("7260839")).PN.	USPAT	OR	OFF	2010/12/21 13:48
S60	3	(("7401230") or ("7421689") or ("7565522")).PN.	USPAT	OR	OFF	2010/12/21 13:51
S61	1291	eros	US-PGPUB; USPAT	OR	ON	2010/12/21 14:13
S62	12	eros and ("726" "713" "380").clas.	US-PGPUB; USPAT	OR	ON	2010/12/21 14:13
S63	0	eros with trust\$3 with window	US-PGPUB; USPAT	OR	ON	2010/12/21 14:14
S64	8	(("4890098") or ("5280579") or ("5502808") or ("5555364") or ("5666030") or ("5673403") or ("5751979") or ("5826013")).PN.	USPAT	OR	OFF	2010/12/21 14:54
S65	11	(("5918039") or ("5978917") or ("5995103") or ("6134661") or ("6167522") or ("6192477") or ("6199181") or ("6216112") or ("6275938") or ("6351816") or ("6385721")).PN.	USPAT	OR	OFF	2010/12/21 14:56
S66	11	(("6480198") or ("6507904") or ("6507948") or ("6546554") or ("6553377") or ("6578140") or ("6581162") or ("6633963") or ("6658573") or ("6663000") or ("6678825")).PN.	USPAT	OR	OFF	2010/12/21 14:58

S67	65	("6678825").URPN.	USPAT	OR	OFF	2010/12/21 14:58
S68	8	("6578140").URPN.	USPAT	OR	OFF	2010/12/21 15:09
S69	4	((("6735700") or ("6321337") or ("7146640") or ("7260839")).PN.	USPAT	OR	OFF	2010/12/21 15:10
S70	5	((("20020066016") or ("20020174349") or ("20030023857") or ("20030097591") or ("20030177397")).PN.	US-PGPUB	OR	OFF	2010/12/21 15:12
S71	6	((("20040006715") or ("20040034794") or ("20040039944") or ("20040054588") or ("20050240810") or ("20060004667")).PN.	US-PGPUB	OR	OFF	2010/12/21 15:13
S72	8	((("6880110") or ("7096381") or ("7577871") or ("7694328") or ("7373505") or ("7039801") or ("7596694") or ("7085928")).PN.	USPAT	OR	OFF	2010/12/21 15:18
S73	11	((("7181768") or ("7284274") or ("6804780") or ("7191469") or ("6505300") or ("7246374") or ("7062672") or ("7444412") or ("6772345") or ("6108715") or ("6873988")).PN.	USPAT	OR	OFF	2010/12/21 15:21
S74	1	"20030131152".pn.	US-PGPUB; USPAT	OR	OFF	2010/12/21 15:23
S75	4522	janus	US-PGPUB; USPAT	OR	OFF	2010/12/21 15:24
S76	1	"7484247".pn.	US-PGPUB; USPAT	OR	OFF	2010/12/21 15:47
S77	0	("7818808").URPN.	USPAT	OR	OFF	2010/12/22 06:08

S78	38	(execut\$3 run\$4) with (web HTML XML content) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:10
S79	2	(execut\$3 run\$4) with (plug\$in applet java\$script embed\$4 near executable) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:15
S80	2	(execut\$3 run\$4 render\$3) with (plug\$in applet java \$script embed\$4 near executable) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:15
S81	4	(execut\$3 run\$4 render\$3) with (malicious virus malware trojan spyware adware) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:17
S82	3	("2005/0005153").URPN.	USPAT	OR	OFF	2010/12/22 06:20
S83	2	(execut\$3 run\$4) with (plug\$in applet java\$script embed\$4 near (content executable)) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:21
S84	0	(execut\$3 run\$4 render\$3) with (separate isolat\$3) near (CPU processor microprocessor) same (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:21
S85	70	(execut\$3 run\$4 render\$3) with (separate isolat\$3) near (CPU processor microprocessor) and (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:21

S86	35	sandbox\$3 with (CPU processor microprocessor) same (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:29
S87	15	sandbox\$3 with (CPU processor microprocessor) and (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) not S86	US-PGPUB; USPAT	OR	ON	2010/12/22 06:30
S88	9	("20050283836" "20030051027" "20060259948" "20060191008" "20060080735" "6785732" "20050131868" "20010032205" "20060101514").pn.	US-PGPUB; USPAT	OR	ON	2010/12/22 06:33
S89	4	(web internet embed\$4) near (video audio content media) with (CPU processor microprocessor) same (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:37
S90	54	("5751979").URPN.	USPAT	OR	OFF	2010/12/22 06:39
S91	67	(web internet embed\$4) near (video audio content media) with (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:41
S92	3	(separate isolat\$3) near (CPU processor microprocessor) with (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:47
S93	5	(execut\$3 run\$4 render\$3) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:56

S94	0	((web internet embed\$4) near (content media video audio page site) web\$site web\$page) with (separate isolat\$3) near (CPU processor microprocessor) same (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:57
S95	3	(separate isolat\$3) near (CPU processor microprocessor) with (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:57
S96	1181	(CPU processor microprocessor) with (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:58
S97	15	(CPU processor microprocessor) with (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:58
S98	15	(CPU processor microprocessor) with (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) not S87	US-PGPUB; USPAT	OR	ON	2010/12/22 06:59

S99	0	(separate special\$4 isolat\$3 individual\$4) with (CPU processor microprocessor) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) not S87	US-PGPUB; USPAT	OR	ON	2010/12/22 07:03
S100	0	(separate special\$4 isolat\$3 individual\$4) with (CPU processor microprocessor) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3 prevent\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:03
S101	31	(CPU processor microprocessor) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3 prevent\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:04
S102	0	(execut\$3 run\$4 render\$3) with (separate isolat\$3) near (CPU processor microprocessor) with sandbox\$3	US-PGPUB; USPAT	OR	ON	2010/12/22 07:11
S103	0	(separate isolat\$3) near (CPU processor microprocessor) with sandbox\$3	US-PGPUB; USPAT	OR	ON	2010/12/22 07:11

S104	36	(CPU processor microprocessor) with sandbox\$3 with (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3 prevent\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:11
S105	11	((("20050198692") or ("20050234856") or ("20060242166") or ("20060242709") or ("20060271835") or ("20080184105") or ("20080178302") or ("20080263358") or ("7562293") or ("7607172") or ("7698559")).PN.	US-PGPUB; USPAT	OR	OFF	2010/12/22 07:14
S106	2	("2005/0198692").URPN.	USPAT	OR	OFF	2010/12/22 07:21
S107	8	("20050198692"   "5832208"   "6092194"   "6240530"   "6675174"   "6701440"   "7171691"   "7263561").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2010/12/22 07:22
S108	54	("5751979").URPN.	USPAT	OR	OFF	2010/12/22 07:24
S109	0	(divid\$3 division split\$4 spread\$3) with (CPU processor microprocessor) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page) same (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:41



S110	7	(divid\$3 division split\$4 spread\$3) with (CPU processor microprocessor) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page) and (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:42
S111	183	(divid\$3 division split\$4 spread\$3) with (CPU processor microprocessor) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:43
S112	61	(execut\$3 run\$4 render\$3 display\$3 reproduc\$3) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page plug\$in script java\$script perl\$script) with (separate isolat\$3 individual second other) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 11:02
S113	9	(execut\$3 run\$4 render\$3 display\$3 reproduc\$3) with (suspicious malicious malware suspect\$2) with (separate isolat\$3 individual second other) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 14:18
S114	68	(execut\$3 run\$4 render\$3 display\$3 reproduc\$3) with (download\$2) with (separate isolat\$3 individual second other) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 14:20
S115	178	("5974549").URPN.	USPAT	OR	OFF	2010/12/28 14:11

S116	1	(CPU processor micro \$processor) with delegat\$3 same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin \$5 check\$3) with (malicious virus malware trojan spyware adware)	USPAT	OR	ON	2010/12/28 14:16
S117	7	(CPU processor micro \$processor) with delegat\$3 and (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin \$5 check\$3) with (malicious virus malware trojan spyware adware)	USPAT	OR	ON	2010/12/28 14:17
S118	8	(CPU processor micro \$processor) with (transfer \$4 delegat\$3 assign\$4) with (task process application) same (protect \$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	USPAT	OR	ON	2010/12/28 14:18
S119	19	("6678712").URPN.	USPAT	OR	OFF	2010/12/28 14:21
S120	8	("6578140").URPN.	USPAT	OR	OFF	2010/12/28 14:27
S121	5	("20060107055"   "20080301670"   "6016546"   "6195587"   "6578140").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2010/12/28 14:27
S122	56	(virus anti\$virus) near (processor co\$processor)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:31
S123	3738	(CPU processor micro \$processor co\$processor video adj processor) with (display\$3 render\$3 reproduc\$4) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:34

S124	1	(CPU processor micro \$processor co\$processor video adj processor) with (display\$3 render\$3 reproduc\$4) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) same (protect \$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:35
S125	14	(CPU processor micro \$processor co\$processor video adj processor) with (display\$3 render\$3 reproduc\$4) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) and (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:35
S126	95	("6199181").URPN.	USPAT	OR	OFF	2010/12/28 14:38
S127	2	("2004/0039944").URPN.	USPAT	OR	OFF	2010/12/28 14:47
S128	14	("6192477").URPN.	USPAT	OR	OFF	2010/12/28 14:48
S129	1	"7146305".pn.	USPAT	OR	OFF	2010/12/28 14:50

S130	235	("20010034847"   "20020032717"   "20020032793"   "20020032880"   "20020035698"   "20020083331"   "20020083334"   "20020138753"   "20020144156"   "20030037136"   "20030088791"   "20030212903"   "20040010718"   "4223380"   "4400769"   "4672609"   "4773028"   "4819234"   "4975950"   "5032979"   "5121345"   "5204966"   "5210704"   "5274824"   "5278901"   "5309562"   "5311593"   "5345595"   "5347450"   "5353393"   "5359659"   "5371852"   "5398196"   "5414833"   "5440723"   "5452442"   "5454074"   "5475839"   "5511184"   "5515508"   "5522026"   "5539659"   "5557742"   "5586260"   "5590331"   "5606668"   "5623600"   "5623601"   "5630061"   "5649095"   "5649185"   "5675711"   "5696486"   "5696822"   "5706210"   "5734697"   "5745692"   "5748098"   "5761504"   "5764887"   "5764890"   "5765030"   "5774727"   "5787177"   "5790799"   "5796942"   "5798706"   "5812763"   "5815574"   "5822517"   "5826013"   "5828833"   "5832208"   "5832211"   "5835726"   "5838903"   "5842002"   "5845067"   "5848233"   "5854916"   "5857191"   "5864665"   "5864803"   "5872978"   "5875296"   "5878420"   "5881236"   "5884033"   "5892903"   "5899999"   "5907834"   "5919257"   "5919258"   "5922051"   "5925126"	US-PGPUB; USPAT; USOCR	OR	OFF	2010/12/28 14:50
------	-----	---	------------------------------	----	-----	---------------------

"5931946" | "5940591" |  
"5950012" | "5961644" |  
"5964839" | "5964889" |  
"5974237" | "5974457" |  
"5978917" | "5983270" |  
"5983348" | "5983350" |  
"5987606" | "5987610" |  
"5987611" | "5991856" |  
"5991881" | "5999711" |  
"5999723" | "6003132" |  
"6006016" | "6009467" |  
"6014645" | "6016553" |  
"6021510").PN. OR  
("6026442" | "6029256" |  
"6035323" | "6035423" |  
"6041347" | "6052709" |  
"6061795" | "6067410" |  
"6070190" | "6070244" |  
"6073172" | "6081894" |  
"6085224" | "6088803" |  
"6088804" | "6092194" |  
"6094731" | "6098173" |  
"6104783" | "6108799" |  
"6118940" | "6119165" |  
"6119234" | "6122738" |  
"6144961" | "6154844" |  
"6161109" | "6167520" |  
"6173413" | "6185689" |  
"6195687" | "6199181" |  
"6205552" | "6226372" |  
"6230288" | "6266773" |  
"6266774" | "6271840" |  
"6272641" | "6275938" |  
"6275942" | "6278886" |  
"6279113" | "6282546" |  
"6298445" | "6301668" |  
"6314520" | "6314525" |  
"6321338" | "6324627" |  
"6324647" | "6324656" |  
"6338141" | "6347374" |  
"6353385" | "6357008" |  
"6377994" | "6396845" |  
"6397242" | "6397245" |  
"6405318" | "6405364" |  
"6408391" | "6415321" |  
"6429952" | "6434615" |  
"6438600" | "6445822" |  
"6453345" | "6453346" |  
"6460141" | "6463426" |  
"6470449" | "6477585" |  
"6477648" | "6477651" |  
"6484203" | "6487666" |  
"6496858" | "6499107" |  
"6510523" | "6517587" |

		"6519647"   "6519703"   "6530024"   "6535227"   "6546493"   "6563959"   "6574737"   "6578147"   "6584454"   "6601190"   "6606744"   "6618501"   "6628824"   "6647139"   "6647400"   "6661904"   "6668082"   "6668084"   "6681331"   "6691232"   "6704874"   "6708212"   "6711127"   "6711615"   "6718383"   "6721806"   "6725377"   "6725378"   "6775780"   "6792144"   "6792546"   "6816973"   "6839850"   "6851057"). PN.				
S131	12	("7146305").URPN.	USPAT	OR	OFF	2010/12/28 14:51
S132	5	restor\$3 with (file application program) with protect\$3 near image	US-PGPUB; USPAT	OR	ON	2010/12/28 17:07

### EAST Search History (I nterference)

< This search history is empty >

**12/ 29/ 10 12:37:10 PM**

**C:\ Documents and Settings\ claforgia\ My Documents\ EAST\ Workspaces\ 12720147.wsp**

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number		12720147
	Filing Date		2010-03-09
	First Named Inventor	Rozman et al.	
	Art Unit	2439	
	Examiner Name	LAFORGIA, CHRISTIAN A	
	Attorney Docket Number	ARAC-01RE1	

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
/CLF/	1	6880110	B2	2005-04-12	Largman et al.		
/CLF/	2	7096381	B2	2006-08-22	Largman et al.		
/CLF/	3	7577871	B2	2009-08-18	Largman et al.		
/CLF/	4	7694328		2010-04-06	Joshi et al.		
/CLF/	5	7373505	B2	2008-05-13	Seltzer et al.		
/CLF/	6	7039801	B2	2006-05-02	Narin		
/CLF/	7	7596694	B1	2009-09-29	Karp et al.		
/CLF/	8	7085928	B1	2006-08-01	Schmid et al.		

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		12720147
Filing Date		2010-03-09
First Named Inventor	Rozman et al.	
Art Unit		2439
Examiner Name	LAFORGIA, CHRISTIAN A	
Attorney Docket Number	ARAC-01RE1	

/CLF/	9	7181768	B1	2007-02-20	Ghosh et al.	
/CLF/	10	7284274	B1	2007-10-16	Walls et al.	
/CLF/	11	6804780	B1	2004-10-12	Touboul	
/CLF/	12	7191469	B2	2007-03-13	Erlingsson	
/CLF/	13	6505300	B2	2003-01-07	Chan et al.	
/CLF/	14	7246374	B1	2007-07-17	Simon et al.	
/CLF/	15	7062672	B2	2006-06-13	Owhadi et al.	
/CLF/	16	7444412	B2	2008-10-28	Owhadi	
/CLF/	17	6772345	B1	2004-08-03	Shetty	
/CLF/	18	6108715		2000-08-22	Leach et al.	
/CLF/	19	6873988	B2	2005-03-25	Herrmann et al.	



**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number	12720147
Filing Date	2010-03-09
First Named Inventor	Rozman et al.
Art Unit	2439
Examiner Name	LAFORGIA, CHRISTIAN A
Attorney Docket Number	ARAC-01RE1

If you wish to add additional U.S. Patent citation information please click the Add button.

**U.S.PATENT APPLICATION PUBLICATIONS**

Examiner Initial*	Cite No	Publication Number	Kind Code <sup>1</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/CLF/	1	20030131152		2003-07-10	Ulfar Erlingsson	

If you wish to add additional U.S. Published Application citation information please click the Add button.

**FOREIGN PATENT DOCUMENTS**

Examiner Initial*	Cite No	Foreign Document Number <sup>3</sup>	Country Code <sup>2</sup> i	Kind Code <sup>4</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T <sup>5</sup>
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button

**NON-PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>5</sup>
/CLF/	1	"SOFTWARE SECURITY AND PRIVACY RISKS IN MOBILE E-COMMERCE" by Anup K. Ghosh and Tara M. Swaminatha, COMMUNICATIONS OF THE ACM February 2001 Vol. 44, No. 2	<input type="checkbox"/>
/CLF/	2	T. Jaeger, A. D. Rubin, and A. Prakash. "Building systems that flexibly control downloaded executable content." In Proceedings of the 1996 USENIX Security Symposium, pages 131-148, San Jose, Ca., 1996.	<input type="checkbox"/>
	3	Nimisha V. Mehta, Karen R. Sollins, "Expanding and Extending the Security Features of Java." Proceedings of the 7th USENIX Security Symposium, San Antonio, Texas, January 26-29, 1998	<input type="checkbox"/>
/CLF/	4	David A. Wagner, "Janus: an approach for confinement of untrusted applications." Master's thesis, University of California, Berkeley, 1999. Also available, Technical Report CSD-99-1056, UC Berkeley, Computer Science Division. <a href="http://www.cs.berkeley.edu/~daw/papers/janus-masters.ps">http://www.cs.berkeley.edu/~daw/papers/janus-masters.ps</a>	<input type="checkbox"/>

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		12720147
Filing Date		2010-03-09
First Named Inventor	Rozman et al.	
Art Unit	2439	
Examiner Name	LAFORGIA, CHRISTIAN A	
Attorney Docket Number	ARAC-01RE1	

/CLF/	5	Richard West and Jason Gloudon, "User-Level Sandboxing: a Safe and Efficient Mechanism for Extensibility", Technical Report, 2003-014, Boston University, June 2003	<input type="checkbox"/>
/CLF/	6	Shaya Potter, Jason Nieh, Dinesh Subhraveti, "Secure Isolation and Migration of Untrusted Legacy Applications." Columbia University Technical Report CUCS-005-04, January 2004	<input type="checkbox"/>
/CLF/	7	M. Schmid, F. Hill, A. Ghosh, "Protecting Data from Malicious Software." Annual Computer Security Applications Conference (ACSAC'02), Las Vegas, NV, December, 2002.	<input type="checkbox"/>
/CLF/	8	Valentin Razmov "Security in Untrusted Code Environments: Missing Pieces of the Puzzle." Dept. of Computer Science and Engineering, University of Washington, March 30, 2002	<input type="checkbox"/>
/CLF/	9	Sotiris Ioannidis and Steven M. Bellovin. "Sub-Operating Systems: A New Approach to Application Security." Technical Report MS-CIS-01-06, University of Pennsylvania, February 2000.	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

**EXAMINER SIGNATURE**

Examiner Signature	/Christian LaForgia/	Date Considered	12/21/2010
--------------------	----------------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> See Kind Codes of USPTO Patent Documents at [www.USPTO.GOV](http://www.USPTO.GOV) or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>3</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>4</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here if English language translation is attached.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number		12720147
	Filing Date		2010-03-09
	First Named Inventor	Rozman, Allen F.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		ARAC-01RE1

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code <sup>1</sup>	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/CLF/	1	4890098	B2	1989-12-26	Dawes, et al	
/CLF/	2	5280579	B2	1994-01-18	Nye	
/CLF/	3	5502808	B2	1996-03-26	Goddard, et al	
/CLF/	4	5555364	B2	1996-09-10	Goldstein	
/CLF/	5	5666030	B2	1997-09-09	Parson	
/CLF/	6	5673403	B2	1997-09-30	Brown, et al	
/CLF/	7	5751979	B2	1998-05-12	McCroy	
/CLF/	8	5826013	B2	1998-10-20	Nachenberg	

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		12720147
Filing Date		2010-03-09
First Named Inventor	Rozman, Allen F.	
Art Unit		
Examiner Name		
Attorney Docket Number		ARAC-01RE1

/CLF/	9	5918039	B2	1999-06-29	Buswell, et al	
/CLF/	10	5978917	B2	1999-11-02	Chi	
/CLF/	11	5995103	B2	1999-11-30	Ashe	
/CLF/	12	6134661	B2	2000-10-07	Topp	
/CLF/	13	6167522	B2	2000-12-26	Lee, et al	
/CLF/	14	6192477	B1	2001-02-20	Corthell	
/CLF/	15	6199181	B1	2001-03-06	Rechef, et al	
/CLF/	16	6216112	B1	2001-04-10	Fuller, et al	
/CLF/	17	6275938	B1	2001-08-14	Bond, et al	
/CLF/	18	6351816	B1	2002-02-26	Mueller, et al	
/CLF/	19	6385721	B1	2002-05-07	Puckette	

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number		12720147
Filing Date		2010-03-09
First Named Inventor	Rozman, Allen F.	
Art Unit		
Examiner Name		
Attorney Docket Number		ARAC-01RE1

/CLF/	20	6480198	B1	2002-11-12	Kang	
/CLF/	21	6507904	B1	2003-01-14	Ellison, et al	
/CLF/	22	6507948	B1	2003-01-14	Curtis, et al	
/CLF/	23	6546554	B1	2003-04-08	Schmidt, et al	
/CLF/	24	6553377	B1	2003-04-22	Eschelbeck, et al	
/CLF/	25	6578140	B1	2003-06-10	Policard	
/CLF/	26	6581162	B1	2003-06-17	Angelo, et al	
/CLF/	27	6633963	B1	2003-10-14	Ellison, et al	
/CLF/	28	6658573	B1	2003-12-02	Bischof	
/CLF/	29	6663000	B1	2003-12-16	Muttick, et al	
/CLF/	30	6678825	B1	2004-01-13	Ellison, et al	

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number	12720147
Filing Date	2010-03-09
First Named Inventor	Rozman, Allen F.
Art Unit	
Examiner Name	
Attorney Docket Number	ARAC-01RE1

/CLF/	31	6735700	B1	2004-05-11	Flint, et al	
/CLF/	32	6321337	B1	2001-11-20	Rechef, et al	
/CLF/	33	7146640	B2	2006-12-05	Goodman, et al	
/CLF/	34	7260839	B2	2007-08-12	Karasaki	

If you wish to add additional U.S. Patent citation information please click the Add button.

[Add](#)

**U.S.PATENT APPLICATION PUBLICATIONS**

[Remove](#)

Examiner Initial*	Cite No	Publication Number	Kind Code <sup>1</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
/CLF/	1	20020066016	A1	2002-05-12	Riordan	
/CLF/	2	20020174349	A1	2002-11-21	Wolff, et al	
/CLF/	3	20030023857	A1	2003-01-30	Hinchcliffe, et al	
/CLF/	4	20030097591	A1	2003-05-22	Pham, et al	
/CLF/	5	20030177397	A1	2003-09-18	Samman	

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**  
( Not for submission under 37 CFR 1.99)

Application Number	12720147
Filing Date	2010-03-09
First Named Inventor	Rozman, Allen F.
Art Unit	
Examiner Name	
Attorney Docket Number	ARAC-01RE1

/CLF/	6	20040006715	A1	2004-01-08	Skrepetos	
/CLF/	7	20040034794	A1	2004-02-19	Mayer, et al	
/CLF/	8	20040039944	A1	2004-02-26	Karasaki	
/CLF/	9	20040054588	A1	2004-03-18	Jacobs, et al	
/CLF/	10	20050240810	A1	2005-10-27	Safford, et al	
/CLF/	11	20060004667	A1	2006-01-05	Neil	

If you wish to add additional U.S. Published Application citation information please click the Add button.

**FOREIGN PATENT DOCUMENTS**

Examiner Initial*	Cite No	Foreign Document Number <sup>3</sup>	Country Code <sup>2</sup> i	Kind Code <sup>4</sup>	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T <sup>5</sup>
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button.

**NON-PATENT LITERATURE DOCUMENTS**

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>5</sup>

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b> ( Not for submission under 37 CFR 1.99)	Application Number		12720147
	Filing Date		2010-03-09
	First Named Inventor	Rozman, Allen F.	
	Art Unit		
	Examiner Name		
	Attorney Docket Number		ARAC-01RE1

/CLF/	1	"Spyware, Adware, and Peer to Peer Networks; The Hidden Threat to Corporate Security" by KEVIN TOWNSEND, Pest Patrol, 2003	<input type="checkbox"/>
/CLF/	2	"Beyond Viruses: Why Anti-Virus Software is No Longer Enough" by DAVID STANG PhD, Pest Patrol, 2002	<input type="checkbox"/>
/CLF/	3	"The Web: Threat or Menace?" from "Firewalls and Internet Security: Repelling the Wiley Hacker", Second Edition, Addison-Wesley, ISBN 0-201-63466-X, 2003	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

**EXAMINER SIGNATURE**

Examiner Signature	/Christian LaForgia/	Date Considered	12/21/2010
--------------------	----------------------	-----------------	------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> See Kind Codes of USPTO Patent Documents at [www.USPTO.GOV](http://www.USPTO.GOV) or MPEP 901.04. <sup>2</sup> Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>3</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>4</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>5</sup> Applicant is to place a check mark here if English language translation is attached.





UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
12/720,147 03/09/2010 Allen F. Rozman ARAC-01RE1 8473

7590 03/09/2011
Allen F. Rozman
6402 Wildlife Trail
Garland, TX 75044

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT PAPER NUMBER

2439

MAIL DATE DELIVERY MODE

03/09/2011

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

<b>Interview Summary</b>	<b>Application No.</b> 12/720,147	<b>Applicant(s)</b> ROZMAN ET AL.	
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439	

All participants (applicant, applicant's representative, PTO personnel):

- (1) Christian LaForgia. (3) \_\_\_\_\_.
- (2) Allen Rozman. (4) \_\_\_\_\_.

Date of Interview: 04 March 2011.

Type: a)  Telephonic b)  Video Conference  
c)  Personal [copy given to: 1)  applicant 2)  applicant's representative]

Exhibit shown or demonstration conducted: d)  Yes e)  No.  
If Yes, brief description: \_\_\_\_\_.

Claim(s) discussed: 1-57.

Identification of prior art discussed: USPN 7,146,305 (van der Made); 6,871,348 (COOPER); 7,024,581 (WANG); 6,578,140 (POLICARD).

Agreement with respect to the claims f)  was reached. g)  was not reached. h)  N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: See Continuation Sheet.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN A NON-EXTENDABLE PERIOD OF THE LONGER OF ONE MONTH OR THIRTY DAYS FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

/Christian LaForgia/  
Primary Examiner, Art Unit 2439

## Summary of Record of Interview Requirements

### Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record

A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

### Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews

Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.

All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

- 1) A brief description of the nature of any exhibit shown or any demonstration conducted,
- 2) an identification of the claims discussed,
- 3) an identification of the specific prior art discussed,
- 4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
- 5) a brief identification of the general thrust of the principal arguments presented to the examiner,  
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
- 6) a general indication of any other pertinent matters discussed, and
- 7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

### Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Continuation of Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: The Applicant discussed the recapture amendments. The examiner stated his position and will review those arguments upon receiving a formal response. The Applicant and Examiner discussed the rejections under 35 USC 112 and 101 and possible amendments to overcome those rejections. Finally, the Applicant and Examiner discussed the prior art rejections, the differences between the prior art and the invention, and possible considerations and amendments to overcome the prior art of record. The Examiner will take action upon receiving a formal response.

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicants: Rozman, *et al.*                      Docket No.: ARAC-01RE1  
Serial No.: 12/720,147                              Filed: 03/09/2010  
Reissue of: 7,484,247                                Issued: January 27, 2009  
Title: System and Method for Protecting a Computer System from Malicious Software.

Commissioner for Patents  
P. O. Box 1450  
Alexandria, VA 22313-1450

**AMENDMENT UNDER 37 CFR §1.111**

Dear Sir:

The following amendments and remarks are presented in response to the Examiner's Office Action mailed January 4, 2011. Please amend the above-referenced application as follows. No new matter has been added.

IN THE SPECIFICATION:

Before the heading “Cross Reference to Related Patents and Applications” kindly insert:

Cross Reference to Multiple Reissue Applications

This application is a reissue application of U.S. Patent No. 7,484,247, entitled “System and Method for Protecting a Computer System from Malicious Software,” issued on January 27, 2009, and is related to another reissue application designated U.S. Patent Application Serial No. 12/720,207 from U.S. Patent No. 7,484,247 filed concurrently herewith, which are incorporated herein by reference. This application is also related to another reissue application designated U.S. Patent Application Serial No. 12/854,149 from U.S. Patent No. 7,484,247 filed on August 10, 2010 and a continuation application therefrom designated U.S. Patent Application Serial No. 13/015,186 filed on January 27, 2011, which are incorporated herein by reference. This application is also related to another reissue application designated U.S. Patent Application Serial No. 12/941,067 from U.S. Patent No. 7,484,247 filed on November 7, 2010, which is incorporated herein by reference.

IN THE CLAIMS:

1. (Twice Amended) A method of operating a computer system capable of exchanging data across a network of one or more computers and having at least a first and second electronic data processor capable of executing instructions using a common operating system, comprising[ the steps of]:

executing browser instructions in a first logical process within the common operating system using the first electronic data processor, wherein the first logical process is capable of accessing data contained in a first memory space[ and a second memory space];

executing instructions in a second logical process within the common operating system using the second electronic data processor, wherein the second logical process is capable of accessing data contained in the second memory space[, the second logical process being further capable of exchanging data across a network of one or more computers]; and

displaying[, in a windowed format on a display terminal,] data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to [the]a display[ terminal];

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second logical process.

2. (Twice Amended) The method of claim 1 wherein the[ first memory space and the] second memory space [comprise separate regions of a common memory space is]comprises

memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

3. (Amended) The method of claim 1 wherein the second logical process [is] comprises a process selected from the group consisting of:

an electronic mail process, an instant messaging process, an internet browser process, an interactive gaming process, a virtual private network (VPN) process, and a reader application process.

4. (Original) The method of claim 1 wherein the first logical process receives user interface data, and passes the user interface data to the second logical process.

5. (Original) The method of claim 1 wherein the first and second electronic data processors are part of a multi-core electronic data processor.

6. (Twice Amended) The method of claim 1 and further comprising[ the step of] restoring at least one corrupted data file[ residing on the second memory space] from [an]a protected image[ residing on the first memory space].

7. (Amended) The method of claim 1 and further comprising[ the step of] automatically deleting at least one data file residing on the second memory space when the second logical process is terminated.

8. (Amended) The method of claim 1 and further comprising[ the steps of]:  
encrypting data with the first logical process;  
transferring the encrypted data from the first logical process to the second logical



process; and

transferring the encrypted data from the second logical process to the network interface device.

9. (Amended) The method of claim 8 and further comprising[ the steps of]:  
decrypting the data with the network interface device; and  
transferring the decrypted data from the network interface device to the network.

10. (Twice Amended) A multi-processor computer system using a common operating system capable of exchanging data across a network of one or more computers via a network interface device, comprising:

a first electronic data processor capable of executing browser instructions using the common operating system and communicatively coupled to a first memory space[ and a second memory space];

a second electronic data processor capable of executing browser instructions using the common operating system and communicatively coupled to [the]a second memory space[ and a network interface device, wherein the second electronic data processor is capable of exchanging data across a network of one or more computers via the network interface device]; and

a video processor adapted to combine video data from the first and second electronic data processors and transmit the combined video data to a display[ terminal for displaying the combines video data in a windowed format];

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing on the second electronic data processor.

11. (Twice Amended) The computer system of claim 10 wherein the [ first memory space and the] second memory space [ comprise separate regions of a common memory space is] comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

12. (Original) The computer system of claim 10 wherein the first and second electronic data processors are part of a dual processor computer system.

13. (Original) The computer system of claim 10 wherein the second electronic data processor and the video processor are co-located on a circuit card, the circuit card being communicatively coupled to the first electronic data processor.

14. (Original) The computer system of claim 10 wherein the computer system is configured such that the first electronic data processor is protected from executing instructions initiated by a malware process downloaded from the network and executing on the second electronic data processor.

15. (Twice Amended) A multi-processor computer system using a common operating system capable of exchanging data across a network of one or more computers, comprising:

at least a first and second electronic data processor capable of executing instructions using the common operating system;

at least a first and second memory space; and

a video processor;

wherein the first and second electronic data processors, first and second memory space,

and video processor are configured to:[for performing the steps of;]

[executing]execute browser instructions in a first logical process with the first electronic data processor, wherein the first logical process is executing within the common operating system and is capable of accessing data contained in the first memory space;

[executing]execute browser instructions in a second logical process with the second electronic data processor, wherein the second logical process is executing within the common operating system and is capable of accessing data contained in the second memory space[, the second logical process being further capable of exchanging data across a network of one or more computers]; and

[displaying, in a windowed format on a display terminal,]display data from the first logical process and the second logical process, wherein the video processor is adapted to combine data from the first and second logical processes and transmit the combined data to [the]a display[ terminal];

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second logical process.

16. (Original) The computer system of claim 15 wherein the computer system is further configured such that the first logical process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second logical process.

17. (Twice Amended) The computer system of claim 15 and further comprising[:] at least one network interface device capable of exchanging data with[ both the second logical

process and with] the network and with a logical process that comprises a process selected from the group consisting of:

the first logical process; and

the second logical process.

18. (Original) The computer system of claim 17 wherein the network interface device is capable of decrypting data received from the second logical process and transmitting the decrypted data to the network while preventing the second logical process from accessing the decrypted data.

19. (Amended) The computer system of claim 15 wherein the at least one electronic data processor [is]comprises a processor selected from the group consisting of[:] a multi-core electronic data processor; dual electronic data processors; and multiple electronic data processors.

20. (Twice Amended) The computer system of claim 15 and further configured to restore[for performing the step of: restoring] at least one corrupted data file[ residing on the second memory space] from [an]a protected image[ residing on the first memory space].

21. (New) A portable computer capable of executing instructions using a common operating system, comprising:

a network interface device configured to exchange data across a network of one or more computers and access at least one website;

at least a first memory space and a second memory space, the first memory space containing at least one system file;

at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, wherein the user interface is

configured to receive input from a computer user;

the at least one electronic data processor configured to execute a first browser process in a first logical process within the common operating system, wherein the first logical process is capable of accessing data contained in the first memory space;

the at least one electronic data processor further configured to execute a second browser process in a second logical process within the common operating system, wherein the second logical process is capable of accessing data contained in the second memory space and is further capable of generating video data from a website accessed via the network; and

a video processor configured to process video data from the second browser process for display;

wherein the first browser process is capable of opening the second browser process and is further capable of passing data to the second browser process;

wherein further the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing within the second browser process.

22. (New) The portable computer of Claim 21 wherein the first browser process is capable of directly exchanging data with the network interface device and with the second browser process.

23. (New) The portable computer of Claim 22 wherein the first browser process is capable of passing data downloaded from the network to the second browser process.

24. (New) The portable computer of Claim 21 wherein the second browser process is capable of directly exchanging data with the network interface device and with the first browser process.

25. (New) The portable computer of Claim 21 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

an Application Specific Integrated Circuit;

a Field Programmable Gate Array;

a plurality of electronic data processors; and

a multi-core electronic data processor.

26. (New) The portable computer of Claim 21 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

27. (New) The portable computer of Claim 21 configured such that at least one corrupted file required for a browser process is capable of being restored from a protected image.

28. (New) The portable computer of Claim 27 wherein the protected image is stored at a location selected from the group consisting of:

a removable drive;

the first memory space;

a partition on a memory device; and

a nonvolatile memory disk.

29. (New) The portable computer of Claim 21 configured such that at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated.

30. (New) The portable computer of Claim 21 configured such that the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.

31. (New) The portable computer of Claim 21 wherein attempts by malware to record data entry by the computer user are effectively blocked.

32. (New) A method of operating a portable computer capable of executing instructions using a common operating system and having at least one electronic data processor communicatively coupled to a first and second memory space and to a network interface device, comprising:

exchanging data across a network of one or more computers with the network interface device and accessing at least one website;

storing at least one system file within the first memory space;

executing a first browser process in a first logical process within the common operating system using the at least one electronic data processor, wherein the first logical process is configured to access data contained in the first memory space;

executing a second browser process in a second logical process within the common operating system using the at least one electronic data processor, wherein the second logical process is configured to access data contained in the second memory space and is further configured to generate video data;

opening the second browser process on instruction from the first browser process;

passing data from the first browser process to the second browser process; and

displaying website video data from the second browser process;

wherein the portable computer is configured such that the at least one system file residing

on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process.

33. (New) The method of Claim 32 wherein the portable computer is configured such that the first browser process is capable of directly exchanging data with the network interface device and with the second browser process.

34. (New) The method of Claim 33 and further comprising downloading data from the network and passing the data from the first browser process to the second browser process.

35. (New) The method of Claim 32 wherein the portable computer is configured such that the second browser process is capable of directly exchanging data with the network interface device and with the first browser process.

36. (New) The method of Claim 32 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

37. (New) The method of Claim 32 and further comprising restoring at least one corrupted file from a protected image.

38. (New) The method of Claim 37 wherein the protected image is stored at a location selected from the group consisting of:

a removable drive;

the first memory space;



a partition on a memory device; and

a nonvolatile memory disk.

39. (New) The method of Claim 32 and further comprising deleting at least one corrupted data file residing on the second memory space when the second logical process is terminated.

40. (New) The method of Claim 32 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

an Application Specific Integrated Circuit;

a Field Programmable Gate Array;

a plurality of electronic data processors; and

a multi-core electronic data processor.

41. (New) The method of Claim 32 wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.

42. (New) The method of Claim 32 and further comprising displaying video data from the first browser process.

43. (New) The method of Claim 32 wherein attempts by malware to record data entry by the computer user are effectively blocked.

44. (New) A method of operating a portable computer comprising a network interface device, at least a first memory space and a second memory space, and at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, comprising:

exchanging data across a network of one or more computers with the network interface

device and accessing at least one website;

storing at least one system file in the first memory space;

opening a first browser process, wherein the first browser process is capable of accessing data contained in the first memory space;

opening a second browser process, wherein the second browser process is capable of accessing data contained in the second memory space, and is further capable of generating data for video display; and

passing data from the first browser process to the second browser process;

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process.

45. (New) The method of Claim 44 wherein the first browser process is capable of directly exchanging data with the network interface device and with the second browser process.

46. (New) The method of Claim 45 and further comprising downloading data from the network and passing the downloaded data from the first browser process to the second browser process.

47. (New) The method of Claim 46 and further comprising storing the downloaded data on the second memory space.

48. (New) The method of Claim 44 wherein the second browser process is capable of directly exchanging data with the network interface device and with the first browser process.

49. (New) The method of Claim 44 and further comprising restoring at least one corrupted file from a protected image.

50. (New) The method of Claim 49 wherein the protected image is stored at a location selected from the group consisting of:

a removable drive;

the first memory space;

a partition on a memory device; and

a non-volatile memory disk.

51. (New) The method of Claim 44 wherein at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated.

52. (New) The method of Claim 44 wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.

53. (New) The method of Claim 44 and further comprising the first browser process instructing the second browser process to open.

54. (New) The method of Claim 44 wherein attempts by malware to record data entry by a computer user are effectively blocked.

55. (New) The method of Claim 44 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

an Application Specific Integrated Circuit;

a Field Programmable Gate Array;

a plurality of electronic data processors; and

a multi-core electronic data processor.

56. (New) The method of Claim 44 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

57. (New) The method of Claim 44 and further comprising the first browser process opening a plurality of second browser processes.

58. (New) The portable computer of Claim 21 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

59. (New) The portable computer of Claim 58 wherein the network comprises a cellular data carrier network.

60. (New) The method of Claim 32 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

61. (New) The method of Claim 60 wherein the network comprises a cellular data carrier network.

62. (New) The method of Claim 44 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

63. (New) The method of Claim 62 wherein the network comprises a cellular data carrier network.

64. (New) A computer program product comprising a program code stored in a non-transitory computer readable medium operable on computer capable of executing instructions using a common operating system and having at least one electronic data processor

communicatively coupled to a first and second memory space and to a network interface device configured to exchange data across a network of one or more computers and access at least one website, configured to:

store at least one system file within the first memory space;

open a first browser process in a first logical process, the first logical process being configured to access data contained in the first memory space;

open a second browser process in a second logical process, the second logical process being configured to access data contained in the second memory space; and

pass data from the first browser process to the second browser process, wherein the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process.

65. (New) The computer program product of Claim 64 wherein the first browser process is capable of opening the second browser process and the program code stored in the non-transitory computer readable medium is further configured to pass data to the second browser process.

66. (New) The computer program product of Claim 64 wherein the second logical process is configured to generate data for display and the program code stored in the non-transitory computer readable medium is further configured to process website video data from the second browser process.

67. (New) The computer program product of Claim 64 wherein the first browser process is capable of directly exchanging data with the network interface device and the second

browser process or the second browser process is capable of directly exchanging data with the network interface device and the first browser process.

68. (New) The computer program product of Claim 64 wherein at least one corrupted file for a browser process is capable of being restored from a protected file.

69. (New) The computer program product of Claim 64 wherein at least one corrupted file residing on the second memory space is capable of being deleted when the second browser process is terminated.

70. (New) The computer program product of Claim 64 wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.

71. (New) The computer program product of Claim 64 wherein attempts by malware to record data entry by a computer user are effectively blocked.

72. (New) The computer program product of Claim 64 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

73. (New) The computer program product of Claim 72 wherein the network comprises a cellular data carrier network.

## Remarks

The Applicants have carefully considered this application in connection with the Examiner's Office Action and respectfully request reconsideration of this application in view of the foregoing amendments and the following remarks. The Applicants thank the Examiner for the Examiner Interview with Mr. Rozman on March 4, 2011 and have taken into consideration the topics of discussion therein when addressing the objections and rejections to this application.

The Applicants originally submitted Claims 1-57 in the application. While Claims 1-3, 6-11, 15, 17, 19-22, 24-26, 28, 32-40, 42, and 44-57 have been amended and Claims 58-73 have been added, no claims have been cancelled herein. For the Examiner's benefit, the Applicants have provided an Appendix II to clearly show the amendments to the specification and claims from the preliminary amendment filed on March 9, 2010. Regarding the added claims, Claims 58-63 depend from previous independent claims, and independent Claim 64 (with its respective dependent Claims 65-73) is a computer program product claim with analogous limitations to ones of the previous independent (and dependent) claims. Also, the Examiner has indicated that Claims 8, 9, 13 and 18 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Accordingly, Claims 1-73 are currently pending in the application.

### **I. Formal Matters**

The Examiner has objected to the information disclosure statement filed 05 August 2010 for failing to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent

document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. In accordance therewith, the Applicants have submitted a copy of “Expanding and Extending the Security Features of Java” to the Examiner, thereby overcoming the objection to the information disclosure statement.

## **II. Rejections under 35 U.S.C. §251**

The Examiner has rejected Claims 1-57 under 35 U.S.C. §251 as being improperly broadened in a reissue application for the recapture of broadened claimed subject matter surrendered in the application for the patent upon which the present reissue is based. The Examiner believes that the claims of the reissue application have been broadened to read on any multiprocessor system capable of exchanging data over a network instead of having a dedicated processor for communicating across the network. The Examiner also believes that the claims of the reissue application have been broadened with the removal of the limitation that the data from both processors are combined to be displayed in a windowed format on a display terminal. The Examiner believes that the removal of the aforementioned claim limitations represents an improper recapture. (Examiner’s Office Action, pp. 2-4.) The Applicants respectfully disagree.

Regarding the first limitation introduced above, the claims of the parent application (U.S. Patent No. 7,484,247) do not include a limitation wherein a processor is dedicated to communicating across a network. Thus, recapture cannot apply to the aforementioned limitation inasmuch as the claims of the parent application do not recite a dedicated processor for communicating across the network. Regarding the windowed format for display, an analogous limitation was present in ones of the claims of the parent application as filed, and was not



amended or argued during prosecution thereof. Thus, this limitation was not previously surrendered during the prosecution of the parent application.

Accordingly, the Applicants believe that recapture does not apply to the present application and respectfully request the Examiner to withdraw the rejection of Claims 1-57 under 35 U.S.C. §251.

### **III. Rejections under 35 U.S.C. §112**

The Examiner has rejected Claims 25 and 44-57 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Applicants have amended ones of Claims 25 and 44-57 to resolve any ambiguities and antecedent basis errors therein, thereby overcoming the rejection of Claims 25 and 44-57 under 35 U.S.C. §112, second paragraph.

### **IV. Rejections under 35 U.S.C. §101**

The Examiner has rejected Claims 44-57 under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. The Applicants have amended ones of Claims 44-57 to direct the claims to a statutory class of invention, thereby overcoming the rejection of Claims 44-57 under 35 U.S.C. §101.

### **V. Rejections under 35 U.S.C. §102**

The Examiner has rejected Claims 32-36, 39-48 and 51-57 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 7,146,305 to van der Made. As the Examiner is no doubt

aware, anticipation requires that each and every limitation of the claimed invention be disclosed in a single prior art reference. The disclosed limitations must either be disclosed expressly or inherently and must be arranged as in the rejected claims.

While the Applicants do not necessarily agree, the Applicants have amended independent Claims 32 and 44 to clarify a previously claimed embodiment of the present application. In accordance therewith, the Applicants believe that van der Made fails to teach or suggest, among other things, a method of operating a portable computer including exchanging data across a network of one or more computers and accessing at least one website as recited in ones of independent Claims 32 and 44 of the present application. It follows that van der Made also fails to teach or suggest executing or opening first and second browser processes as recited in ones of independent Claims 32 and 44 of the present application for the reasons as set forth below.

Van der Made is directed to “a virtual machine system for computer code behavior analysis, the virtual machine system having a software processor.” (Column 3, lines 8-10.) Van der Made is clear that the virtual machine system is directed to a system that analyzes application program code for malware, and does so in a simulated, virtual machine environment. Van der Made teaches:

The analytical virtual machine (AVM) described here is intended to be used in automated code function analysis and behavior extraction. (Column 4, lines 24-26.)

Van der Made further teaches:

The preceding discussion described a virtual machine that performs analysis of an application program (code) within a protected execution environment on a real computer. (Column 10, lines 29-31.)

In accordance with the teaching of van der Made, the Applicants respectfully assert that the virtual machine is not intended to exchange data across a network of one or more computers.

As van der Made provides:

Preferred implementations of an analytical virtual machine do not allow physical input or output to take place or any interaction between the program code under analysis and the real or physical computer system. Instead, input and output operations, system calls and instructions are simulated in a manner transparent to the code under analysis. (Column 4, lines 8-14.)

Van der Made goes on to reiterate the intent that no interactions be allowed between the program code under analysis and the real or physical system by stating:

No direct interaction is allowed to exist between the application program and the system software execution environment and/or the computer hardware. (Column 10, lines 42-44.)

The Applicants assertion that van der Made teaches a system for computer code simulation and behavior analysis is further illustrated by a statement in van der Made that:

The aim of execution within the AVM is to perform an analysis that extracts the program code behavior under every condition contained within that program. Once this aim has been satisfied, the analytical virtual machine is terminated, preserving the generated behavior pattern and the sequencer structure, which contains the sequence in which events recorded in the behavior pattern have taken place. (Column 10, line 63 to column 11, line 3.)

Van der Made then teaches that the end product of the Analytical Virtual Machine (AVM) is by stating:

The end product of an invocation of an AVM in accordance with preferred embodiments of the present invention are the contents of the behavior flag register and the sequencer. (Column 10, lines 7-10.)

Thus, it is quite clear from the excerpts of the reference reproduced above that van der Made fails to teach or suggest a method of operating a portable computer including exchanging data across a network of one or more computers and accessing at least one website as recited in ones of independent Claims 32 and 44 of the present application. To reiterate, van der Made is directed to a virtual machine system for computer code behavior analysis, whereas the method of operating the portable computer as recited in ones of independent Claims 32 and 44 of the present application is operable to interact with a network interface device to exchange data across a network of one or more computers, execute or open browser processes and, ultimately, protect a system file residing on a memory space from corruption by a malware process.

Thus, van der Made fails to teach or suggest the limitations of Claims 32 and 44, and the claims dependent thereon. Accordingly, the Applicants respectfully request the Examiner to withdraw the §102 rejection in view thereof with respect to Claims 32-36, 39-48 and 51-57 of the present application.

## **VI. Rejections under 35 U.S.C. §103(a)**

The Examiner has rejected Claims 1-5, 7, 10, 11 and 14-17 under 35 U.S.C. § 103(a) as being unpatentable over van der Made in view of U.S. Patent No. 6,871,348 to Cooper. The Examiner has also rejected Claims 6 and 20 under 35 U.S.C. § 103(a) as being unpatentable over van der Made in view of Cooper and further in view of U.S. Patent No. 7,024,581 to Wang, *et al.* (“Wang”). The Examiner has also rejected Claims 12 and 19 under 35 U.S.C. § 103(a) as being unpatentable over van der Made in view of Cooper and further in view of U.S. Patent No. 6,578,140 to Pollicard. The Examiner has also rejected Claims 21-26 and 29-31 under 35 U.S.C.

§ 103(a) as being unpatentable over van der Made. The Examiner has also rejected Claims 27, 28, 37, 38 and 50 under 35 U.S.C. § 103(a) as being unpatentable over van der Made in view of Wang.

With respect to independent Claims 1, 10, 15 and 21 of the present application, the Examiner relies on van der Made for exchanging data across a network of one or more computers. (Examiner's Office Action, pp. 13, 14, 16, 17 and 20-22.) For the reasons as set forth above, the Applicants respectfully disagree. To reiterate, van der Made is directed to a virtual machine system for computer code behavior analysis, whereas the method of operating a portable computer as recited in independent Claim 1, the multi-processor computer systems as recited in ones of independent Claims 10 and 15, and a portable computer as recited in independent Claim 21 of the present application are configured to exchange data across a network of one or more computers, execute browser processes or instructions and, ultimately, protect data or a system file residing on a memory space from corruption by a malware process. The same, of course, is true for the method of operating the portable computer as recited in ones of independent Claims 32 and 44 of the present application.

In accordance therewith, it appears to the Applicants that van der Made (and the other references by the Examiner's own admission) does not teach or suggest, among other things, a computer, or related method of operating the same, configured to exchange data across a network of one or more computers as recited in ones of independent Claims 1, 10, 15, 21, 32 and 44 of the present application. Thus, the combination of references does not teach or suggest all of the limitations of independent Claims 1, 10, 15, 21, 32 and 44 of the present application. In view of the foregoing remarks, the cited references do not support the Examiner's rejection of independent Claims 1, 10, 15, 21, 32 and 44 and the claims dependent thereon, namely, Claims

2-7, Claims 11, 12, 14, Claims 16, 17, 19, 20, Claims 22-31, Claims 37, 38, and Claim 50, respectively, under 35 U.S.C. §103(a). In accordance therewith, the Applicants respectfully request the Examiner withdraw the rejection.

## VII. Conclusion

In view of the foregoing amendments and remarks, the Applicants now see all of the claims currently pending in this application to be in condition for allowance and therefore earnestly solicit a Notice of Allowance therefor.

The Applicants request that the Examiner telephone the undersigned attorney of record at (972) 732-1001 if such would further expedite the prosecution of the present application. The Commissioner is hereby authorized to charge any additional fees, or credit any overpayments, to Deposit Account No. 50-1065.

Respectfully submitted,

\_\_\_\_\_  
April 4, 2011

Date

\_\_\_\_\_  
/Glenn W. Boisbrun/

Glenn W. Boisbrun  
Attorney for Applicant  
Reg. No. 39,615

Slater & Matsil, L.L.P.  
17950 Preston Rd., Suite 1000  
Dallas, Texas 75252-5793  
Tel. 972-732-1001  
Fax: 972-732-9218

**APPENDIX I**

**STATUS OF CLAIMS AND  
SUPPORT FOR CLAIM CHANGES**

<b>Claims</b>	<b>Status</b>	<b>Support</b>		
1	Twice Amended	Col 9 lines 30-37 Fig. 1, 190, 195 Col 18 lines 3-5	Col 11 lines 2-4 Fig. 1, 120, 191, 190, 110, 130	Col 6 lines 56-60 Col 10 line 67
2	Twice Amended	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
3	Amended	Col 18 lines 33-38		
4	Original			
5	Original			
6	Twice Amended	Fig. 4, 420	Col 12 lines 46-58	
7	Amended	Col 18 lines 49-52		
8	Amended	Col 18 lines 53-60		
9	Amended	Col 18 lines 61-65		
10	Twice Amended	Col 9 lines 30-37 Fig. 1, 190, 195 Col 18 lines 3-5	Col 11 lines 2-4 Fig. 1, 120, 191, 190, 110, 130	Col 6 lines 56-60 Col 10 line 67
11	Twice Amended	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
12	Original			
13	Original			
14	Original			
15	Twice Amended	Col 9 lines 30-37 Fig. 1, 190, 195	Col 11 lines 2-4 Fig. 1, 120, 191, 190, 110, 130	Col 6 lines 56-60 Col 10 line 67
16	Original			
17	Twice Amended	Fig. 1, 120, 191, 190, 110, 130		
18	Original			
19	Amended	Col 20 lines 38-42		
20	Twice Amended	Fig. 4, 420	Col 12 lines 46-58	
21	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53 Fig. 1, 120, 191, 190, 110, 130	Fig. 1, 120, 150, 160 Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Col 11 lines 2-4 Col 8 lines 1-6	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 23-28 Col 18 lines 3-5
22	New	Fig. 1, 120, 191, 190		
23	New	Fig. 1, 120, 191,	Col 11 lines 38-41	

		190, 195		
24	New	Fig. 1, 140, 190		
25	New	Col 14 lines 62-67	Col 9 lines 30-47	
26	New	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
27	New	Fig. 4, 420	Col 12 lines 46-58	
28	New	Col 12 lines 46-58	Col 7 lines 13-16	
29	New	Col 8 lines 23-26		
30	New	Col 19 lines 33-37		
31	New	Col 7 lines 58-62		
32	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Col 11 lines 2-4 Col 8 lines 1-6	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 23-28
33	New	Fig. 1, 120, 191, 190		
34	New	Fig. 1, 120, 191, 190, 195	Col 11 lines 38-41	
35	New	Fig. 1, 140, 190		
36	New	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
37	New	Fig. 4, 420	Col 12 lines 46-58	
38	New	Col 12 lines 46-58	Col 7 lines 13-16	
39	New	Col 8 lines 23-26		
40	New	Col 14 lines 62-67	Col 9 lines 30-47	
41	New	Col 19 lines 33-37		
42	New	Fig. 1, 120, 170, 171, 180		
43	New	Col 7 lines 58-62		
44	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Col 11 lines 2-4 Col 8 lines 1-6	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 25-28
45	New	Fig. 1, 120, 191, 190		
46	New	Fig. 1, 120, 191, 190, 195	Col 11 lines 38-41	
47	New	Fig. 3, 320		
48	New	Fig. 1, 140, 190		
49	New	Fig. 4, 420	Col 12 lines 46-58	
50	New	Col 12 lines 46-58	Col 7 lines 13-16	
51	New	Col 8 lines 23-26		
52	New	Col 19 lines 33-37		



53	New	Fig 2, 220		
54	New	Col 7 lines 58-62		
55	New	Col 14 lines 62-67	Col 9 lines 30-47	
56	New	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
57	New	Col 13 lines 22-24	Fig 2, 220	
58	New	Col 10 lines 19-22		
59	New	Col 1 and 2	US PAT 6,216,112	
60	New	Col 10 lines 19-22		
61	New	Col 1 and 2	US PAT 6,216,112	
62	New	Col 10 lines 19-22		
63	New	Col 1 and 2	US PAT 6,216,112	
64	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Col 11 lines 2-4 Col 8 lines 1-6	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 25-28
65	New	Fig. 1, 120, 191, 190, 195	Col 11 lines 38-41 Col 13 lines 22-24	Fig 2, 220
66	New	Fig. 1		
67	New	Fig. 1, 120, 191, 190		
68	New	Fig. 4, 420	Col 12 lines 46-58	
69	New	Col 8 lines 23-26		
70	New	Col 19 lines 33-37		
71	New	Col 7 lines 58-62		
72	New	Col 10 lines 19-22		
73	New	Col 1 and 2	US PAT 6,216,112	

## APPENDIX II

### SPECIFICATION AS AMENDED ACCORDING TO STANDARD AMENDMENT FORMAT

Kindly amend the “Cross Reference to Multiple Reissue Applications” section as set forth below:

#### Cross Reference to Multiple Reissue Applications

This application is a reissue application of U.S. Patent No. 7,484,247, entitled “System and Method for Protecting a Computer System from Malicious Software,” issued on January 27, 2009, and is related to another reissue application designated U.S. Patent Application Serial No. 12/720,207 ~~\_\_\_\_\_ (Docket No. ARAC-01RE2)~~ from U.S. Patent No. 7,484,247 filed concurrently herewith, which are incorporated herein by reference. This application is also related to another reissue application designated U.S. Patent Application Serial No. 12/854,149 from U.S. Patent No. 7,484,247 filed on August 10, 2010 and a continuation application therefrom designated U.S. Patent Application Serial No. 13/015,186 filed on January 27, 2011, which are incorporated herein by reference. This application is also related to another reissue application designated U.S. Patent Application Serial No. 12/941,067 from U.S. Patent No. 7,484,247 filed on November 7, 2010, which is incorporated herein by reference.

## CLAIMS AS AMENDED ACCORDING TO STANDARD AMENDMENT FORMAT

1. (Currently Amended) A method of operating a computer system capable of exchanging data across a network of one or more computers and having at least a first and second electronic data processor capable of executing instructions using a common operating system, comprising ~~the steps of:~~

executing browser instructions in a first logical process within the common operating system using the first electronic data processor, wherein the first logical process is capable of accessing data contained in a first memory space;

executing instructions in a second logical process within the common operating system using the second electronic data processor, wherein the second logical process is capable of accessing data contained in the second memory space; and

displaying data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to a display;

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second logical process.

2. (Currently Amended) The method of claim 1 wherein the second memory space [[is]]comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;  
random access memory (RAM); and  
both volatile and nonvolatile memory.

3. (Currently Amended) The method of claim 1 wherein the second logical process  
[[is]]comprises a process selected from the group consisting of:

an electronic mail process, an instant messaging process, an internet browser process, an  
interactive gaming process, a virtual private network (VPN) process, and a reader application  
process.

4. (Previously Presented) The method of claim 1 wherein the first logical process  
receives user interface data, and passes the user interface data to the second logical process.

5. (Previously Presented) The method of claim 1 wherein the first and second  
electronic data processors are part of a multi-core electronic data processor.

6. (Currently Amended) The method of claim 1 and further comprising ~~the step of~~  
restoring at least one corrupted data file from a protected image.

7. (Currently Amended) The method of claim 1 and further comprising ~~the step of~~  
automatically deleting at least one data file residing on the second memory space when the  
second logical process is terminated.

8. (Currently Amended) The method of claim 1 and further comprising ~~the steps of~~:  
encrypting data with the first logical process;  
transferring the encrypted data from the first logical process to the second logical  
process; and  
transferring the encrypted data from the second logical process to the network interface  
device.

9. (Currently Amended) The method of claim 8 and further comprising ~~the steps of:~~  
decrypting the data with the network interface device; and  
transferring the decrypted data from the network interface device to the network.

10. (Currently Amended) A multi-processor computer system using a common operating system capable of exchanging data across a network of one or more computers via a network interface device, comprising:

a first electronic data processor capable of executing browser instructions using the common operating system and communicatively coupled to a first memory space;

a second electronic data processor capable of executing browser instructions using the common operating system and communicatively coupled to a second memory space; and

a video processor adapted to combine video data from the first and second electronic data processors and transmit the combined video data to a display;

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing on the second electronic data processor.

11. (Currently Amended) The computer system of claim 10 wherein the second memory space [[is]]comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

12. (Previously Presented) The computer system of claim 10 wherein the first and second electronic data processors are part of a dual processor computer system.

13. (Previously Presented) The computer system of claim 10 wherein the second electronic data processor and the video processor are co-located on a circuit card, the circuit card being communicatively coupled to the first electronic data processor.

14. (Previously Presented) The computer system of claim 10 wherein the computer system is configured such that the first electronic data processor is protected from executing instructions initiated by a malware process downloaded from the network and executing on the second electronic data processor.

15. (Currently Amended) A multi-processor computer system using a common operating system capable of exchanging data across a network of one or more computers, comprising:

at least a first and second electronic data processor capable of executing instructions using the common operating system;

at least a first and second memory space; and

a video processor;

wherein the first and second electronic data processors, first and second memory space, and video processor are configured to:~~for performing the steps of;~~

~~executing~~execute browser instructions in a first logical process with the first electronic data processor, wherein the first logical process is executing within the common operating system and is capable of accessing data contained in the first memory space;

~~executing~~execute browser instructions in a second logical process with the second electronic data processor, wherein the second logical process is executing within the common

operating system and is capable of accessing data contained in the second memory space; and  
~~displaying~~display data from the first logical process and the second logical  
process, wherein the video processor is adapted to combine data from the first and second logical  
processes and transmit the combined data to a display;

wherein the computer system is configured such that the second electronic data processor  
is operating in a protected mode and data residing on the first memory space is protected from  
corruption by a malware process downloaded from the network and executing as part of the  
second logical process.

16. (Previously Presented) The computer system of claim 15 wherein the computer  
system is further configured such that the first logical process is protected from executing  
instructions initiated by a malware process downloaded from the network and executing as part  
of the second logical process.

17. (Currently Amended) The computer system of claim 15 and further  
comprising[[:]] at least one network interface device capable of exchanging data with the  
network and with a logical process that comprises a process selected from the group consisting  
of:

the first logical process; and

the second logical process.

18. (Previously Presented) The computer system of claim 17 wherein the network  
interface device is capable of decrypting data received from the second logical process and  
transmitting the decrypted data to the network while preventing the second logical process from  
accessing the decrypted data.

19. (Currently Amended) The computer system of claim 15 wherein the at least one electronic data processor ~~[[is]]~~comprises a processor selected from the group consisting of~~[[:]]~~ a multi-core electronic data processor; dual electronic data processors; and multiple electronic data processors.

20. (Currently Amended) The computer system of claim 15 and further configured to restore~~for performing the step of: restoring~~ at least one corrupted data file from a protected image.

21. (Currently Amended) A portable computer capable of executing instructions using a common operating system, comprising:

a network interface device configured to exchange data across a network of one or more computers ~~using a wireless connection~~and access at least one website;

at least a first memory space and a second memory space, the first memory space containing at least one system file;

at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, wherein the user interface is configured to receive input from a computer user;

the at least one electronic data processor configured to execute a first browser process in a first logical process within the common operating system, wherein the first logical process is capable of accessing data contained in the first memory space;

the at least one electronic data processor further configured to execute a second browser process in a second logical process within the common operating system, wherein the second logical process is capable of accessing data contained in the second memory space and is further capable of generating video data from a website accessed via the network; and



a video processor configured to ~~transmit~~process video data from the second browser process ~~to a~~for display;

wherein the first browser process is capable of opening the second browser process and is further capable of passing data to the second browser process;

wherein further the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing within the second browser process.

22. (Currently Amended) The portable computer of Claim 21 wherein the first browser process is capable of directly exchanging data with the network interface device and with the second browser process.

23. (Previously Presented) The portable computer of Claim 22 wherein the first browser process is capable of passing data downloaded from the network to the second browser process.

24. (Currently Amended) The portable computer of Claim 21 wherein the second browser process is capable of directly exchanging data with the network interface device and with the first browser process.

25. (Currently Amended) The portable ~~wireless communication device~~computer of Claim 21 wherein the at least one electronic data processor ~~[[is]]~~comprises a processor selected from the group consisting of:

an Application Specific Integrated Circuit;

a Field Programmable Gate Array;

a plurality of electronic data processors; and

a multi-core electronic data processor.

26. (Currently Amended) The portable computer of Claim 21 wherein the second memory space ~~[[is]]~~comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

27. (Previously Presented) The portable computer of Claim 21 configured such that at least one corrupted file required for a browser process is capable of being restored from a protected image.

28. (Currently Amended) The portable computer of Claim 27 wherein the protected image is stored at a location selected from the group consisting of:

a removable drive;

the first memory space;

a partition on a memory device; and

a nonvolatile memory disk;

~~another device.~~

29. (Previously Presented) The portable computer of Claim 21 configured such that at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated.

30. (Previously Presented) The portable computer of Claim 21 configured such that the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.

31. (Previously Presented) The portable computer of Claim 21 wherein attempts by malware to record data entry by the computer user are effectively blocked.

32. (Currently Amended) A method of operating a portable computer capable of executing instructions using a common operating system and having at least one electronic data processor communicatively coupled to a first and second memory space and to a network interface device, ~~wherein the network interface device is configured to exchange data across a network of one or more computers using a wireless connection,~~ comprising the steps of:

exchanging data across a network of one or more computers with the network interface device and accessing at least one website;

storing at least one system file within the first memory space;

executing a first browser process in a first logical process within the common operating system using the at least one electronic data processor, wherein the first logical process is configured to access data contained in the first memory space;

executing a second browser process in a second logical process within the common operating system using the at least one electronic data processor, wherein the second logical process is configured to access data contained in the second memory space and is further configured to generate video data;

opening the second browser process on instruction from the first browser process;

passing data from the first browser process to the second browser process; and

displaying website video data from the second browser process;

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process.

33. (Currently Amended) The method of Claim 32 wherein the portable computer is configured such that the first browser process is capable of directly exchanging data with the network interface device and with the second browser process.

34. (Currently Amended) The method of Claim 33 and further comprising ~~the step~~ ~~of:~~  
——downloading data from the network and passing the data from the first browser process to the second browser process.

35. (Currently Amended) The method of Claim 32 wherein the portable computer is configured such that the second browser process is capable of directly exchanging data with the network interface device and with the first browser process.

36. (Currently Amended) The method of Claim 32 wherein the second memory space ~~comprises~~ memory selected from the group consisting of:

- a memory zone within a physical memory common to the first memory space;
- a partition on a memory device;
- random access memory (RAM); and
- both volatile and nonvolatile memory.

37. (Currently Amended) The method of Claim 32 and further comprising ~~the step~~ ~~of:~~  
——restoring at least one corrupted file from a protected image.

38. (Currently Amended) The method of Claim 37 wherein the protected image is stored at a location selected from the group consisting of:

- a removable drive;
- the first memory space;

a partition on a memory device; and

a nonvolatile memory disk;

~~another device.~~

39. (Currently Amended) The method of Claim 32 and further comprising ~~the step~~  
~~of:~~

~~deleting at least one corrupted data file residing on the second memory space when the~~  
~~second logical process is terminated.~~

40. (Currently Amended) The method of Claim 32 wherein the at least one electronic  
data processor ~~[[is]]~~ comprises a processor selected from the group consisting of:

an Application Specific Integrated Circuit;

a Field Programmable Gate Array;

a plurality of electronic data processors; and

a multi-core electronic data processor.

41. (Previously Presented) The method of Claim 32 wherein the first browser process  
is protected from executing instructions initiated by a malware process downloaded from the  
network and executing as part of the second browser process.

42. (Currently Amended) The method of Claim 32 and further comprising ~~the step~~  
~~of:~~

~~displaying video data from the first browser process.~~

43. (Previously Presented) The method of Claim 32 wherein attempts by malware to  
record data entry by the computer user are effectively blocked.

44. (Currently Amended) A method of operating a portable computer[[,]] comprising  
a network interface device ~~configured to exchange data across a network of one or more~~

~~computers using a wireless connection~~, at least a first memory space and a second memory space, and at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, ~~wherein the user interface is configured to receive input from a computer user, wherein the portable computer is configured for performing the steps of~~comprising:

exchanging data across a network of one or more computers with the network interface device and accessing at least one website;

storing at least one system file in the first memory space;

opening a first browser process, wherein the first browser process is capable of accessing data contained in the first memory space;

opening a second browser process, wherein the second browser process is capable of accessing data contained in the second memory space, and is further capable of generating ~~video~~ data for video display; and

passing data from the first browser process to the second browser process;

~~displaying video data from the second browser process;~~

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process.

45. (Currently Amended) The ~~portable computer~~method of Claim 44 wherein the first browser process is capable of directly exchanging data with the network interface device and with the second browser process.

46. (Currently Amended) The ~~portable computer~~method of Claim 45 and further comprising ~~configured for performing the step of:~~

——downloading data from the network and passing the downloaded data from the first browser process to the second browser process.

47. (Currently Amended) The ~~portable computer~~method of Claim 46 and further comprising ~~configured for performing the step of:~~

——storing the downloaded data on the second memory space.

48. (Currently Amended) The ~~portable computer~~method of Claim 44 wherein the second browser process is capable of directly exchanging data with the network interface device and with the first browser process.

49. (Currently Amended) The ~~portable computer~~method of Claim 44 and further comprising ~~configured for performing the step of:~~

——restoring at least one corrupted file from a protected image.

50. (Currently Amended) The ~~portable computer~~method of Claim 49 wherein the protected image is stored at a location selected from the group consisting of:

a removable drive;

the first memory space;

a partition on a memory device; and

a non-volatile memory disk;

——~~another device.~~

51. (Currently Amended) The ~~portable computer~~method of Claim 44 ~~configured such that~~wherein at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated.

52. (Currently Amended) The ~~portable computer~~method of Claim 44 wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.

53. (Currently Amended) The ~~portable computer~~method of Claim 44 and further comprising configured for performing the step of:  
——the first browser process instructing the second browser process to open.

54. (Currently Amended) The ~~portable computer~~method of Claim 44 wherein attempts by malware to record data entry by [[the]]a computer user are effectively blocked.

55. (Currently Amended) The ~~portable computer~~method of Claim 44 wherein the at least one electronic data processor [[is]]comprises a processor selected from the group consisting of:

- an Application Specific Integrated Circuit;
- a Field Programmable Gate Array;
- a plurality of electronic data processors; and
- a multi-core electronic data processor.

56. (Currently Amended) The ~~portable computer~~method of Claim 44 wherein the second memory space [[is]]comprises memory selected from the group consisting of:

- a memory zone within a physical memory common to the first memory space;
- a partition on a memory device;
- random access memory (RAM); and
- both volatile and nonvolatile memory.



57. (Currently Amended) The ~~portable computer~~method of Claim 44 and further comprising configured for performing the step of:

——the first browser process opening a plurality of second browser processes.

58. (New) The portable computer of Claim 21 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

59. (New) The portable computer of Claim 58 wherein the network comprises a cellular data carrier network.

60. (New) The method of Claim 32 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

61. (New) The method of Claim 60 wherein the network comprises a cellular data carrier network.

62. (New) The method of Claim 44 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

63. (New) The method of Claim 62 wherein the network comprises a cellular data carrier network.

64. (New) A computer program product comprising a program code stored in a non-transitory computer readable medium operable on computer capable of executing instructions using a common operating system and having at least one electronic data processor communicatively coupled to a first and second memory space and to a network interface device configured to exchange data across a network of one or more computers and access at least one website, configured to:

store at least one system file within the first memory space;

open a first browser process in a first logical process, the first logical process being

configured to access data contained in the first memory space;

open a second browser process in a second logical process, the second logical process being configured to access data contained in the second memory space; and

pass data from the first browser process to the second browser process, wherein the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process.

65. (New) The computer program product of Claim 64 wherein the first browser process is capable of opening the second browser process and the program code stored in the non-transitory computer readable medium is further configured to pass data to the second browser process.

66. (New) The computer program product of Claim 64 wherein the second logical process is configured to generate data for display and the program code stored in the non-transitory computer readable medium is further configured to process website video data from the second browser process.

67. (New) The computer program product of Claim 64 wherein the first browser process is capable of directly exchanging data with the network interface device and the second browser process or the second browser process is capable of directly exchanging data with the network interface device and the first browser process.

68. (New) The computer program product of Claim 64 wherein at least one corrupted file for a browser process is capable of being restored from a protected file.

69. (New) The computer program product of Claim 64 wherein at least one corrupted file residing on the second memory space is capable of being deleted when the second browser process is terminated.

70. (New) The computer program product of Claim 64 wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.

71. (New) The computer program product of Claim 64 wherein attempts by malware to record data entry by a computer user are effectively blocked.

72. (New) The computer program product of Claim 64 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

73. (New) The computer program product of Claim 72 wherein the network comprises a cellular data carrier network.

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicants: Rozman, *et al.* Docket No.: ARAC-01RE1  
Serial No.: 12/720,147 Art Unit: 2439  
Filed: March 9, 2010 Examiner: Christian A. LaForgia  
Title: System and Method for Protecting a Computer System from Malicious Software

Commissioner for Patents  
P. O. Box 1450  
Alexandria, VA 22313-1450

**INFORMATION DISCLOSURE STATEMENT**

Dear Sir:

The Applicants wish to bring to the attention of the U.S. Patent and Trademark Office the information noted on the enclosed form PTO/SB/08b, which may be considered material to the examination of the above-identified application. Applicants have included a copies of the non-patent literature.

This Information Disclosure Statement is submitted under 37 C.F.R. §1.97(c) together with a \$180.00 fee under 37 C.F.R. §1.17(p) after the C.F.R. §1.97(b) time period, but before final action or notice of allowance, whichever occurs first.

Please charge the required fee of \$180.00 and any additional amount, or credit any overpayment to Deposit Acct. No. 50-1065 of the below mentioned firm.

Respectfully submitted,

April 4, 2011

Date

/Glenn W. Boisbrun/

Glenn W. Boisbrun  
Attorney for Applicants  
Reg. No. 39,615

Slater & Matsil, L.L.P.  
17950 Preston Road, Suite 1000  
Dallas, Texas 75252  
Tel: (972) 732-1001  
Fax: (972) 732-9218



## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	12720147
<b>Filing Date:</b>	09-Mar-2010
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Filer:</b>	Glenn W. Boisbrun/Jill Errera
<b>Attorney Docket Number:</b>	ARAC-01RE1

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
Claims in excess of 20	2202	16	26	416
Independent claims in excess of 3	2201	1	110	110

### Miscellaneous-Filing:

**Petition:**

**Patent-Appeals-and-Interference:**

**Post-Allowance-and-Post-Issuance:**

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Extension-of-Time:</b>				
<b>Miscellaneous:</b>				
Submission- Information Disclosure Stmt	1806	1	180	180
<b>Total in USD (\$)</b>				<b>706</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	9805675
<b>Application Number:</b>	12720147
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	8473
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Correspondence Address:</b>	Allen F. Rozman - 6402 Wildlife Trail - Garland TX 75044 US 214-478-2172 arozman@verizon.net
<b>Filer:</b>	Glenn W. Boisbrun/Jill Errera
<b>Filer Authorized By:</b>	Glenn W. Boisbrun
<b>Attorney Docket Number:</b>	ARAC-01RE1
<b>Receipt Date:</b>	04-APR-2011
<b>Filing Date:</b>	09-MAR-2010
<b>Time Stamp:</b>	17:35:26
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$706



RAM confirmation Number	4458
Deposit Account	501065
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

- Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)
- Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)
- Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)
- Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)
- Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		ARAC-01RE1_Amendment.pdf	210206 3042a75fb144d159faccad7803ca80b5775d99be	yes	47

**Multipart Description/PDF files in .zip description**

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Specification	2	2
Claims	3	18
Applicant Arguments/Remarks Made in an Amendment	19	47

**Warnings:**

**Information:**

2	Transmittal Letter	ARAC-01RE1_IDS_Letter.pdf	81062 d42619d80f2cab517c2e86bf8da4dd7998b5381b	no	1
---	--------------------	---------------------------	---	----	---

**Warnings:**

**Information:**

3	Information Disclosure Statement (IDS) Filed (SB/08)	ARAC-01RE1_IDS.pdf	114939 eebc8d460ea7d249d9612cca0cf9824bb425651c	no	1
---	--	--------------------	--	----	---

**Warnings:**

**Information:**

This is not an USPTO supplied IDS fillable form

4	NPL Documents	ARAC-01RE1_NPL.pdf	2262209 29ba1b2a347a3cf80d716045da236272740299ee	no	15
---	---------------	--------------------	---	----	----

**Warnings:**

**Information:**

5	Fee Worksheet (PTO-875)	fee-info.pdf	33672 000da43d4b0adf40768e1d5e710ac9d78a54d6fc	no	2
---	-------------------------	--------------	---	----	---

**Warnings:**

**Information:**

<b>Total Files Size (in bytes):</b>	2702088
-------------------------------------	---------

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number <b>12/720,147</b>	Filing Date <b>03/09/2010</b>	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (j), or (m))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A		N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(j))</small>	minus 20 =	*	X \$ =	OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =		X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>						
			TOTAL		TOTAL	

\* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT	<b>04/04/2011</b>	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 73	Minus ** 57	= 16	X \$26 =	416	OR	X \$ =
	Independent (37 CFR 1.16(h))	* 6	Minus ***6	= 0	X \$110 =	0	OR	X \$ =
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR	
					TOTAL ADD'L FEE	<b>416</b>	OR	TOTAL ADD'L FEE

	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	X \$ =		OR	X \$ =
	Independent (37 CFR 1.16(h))	*	Minus ***	=	X \$ =		OR	X \$ =
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:  
 /BRUCE HARRISON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number <b>12/720,147</b>	Filing Date <b>03/09/2010</b>	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR			
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (j), or (m))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A			N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(j))</small>	minus 20 =	*	X \$ =		OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =			X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>							
			TOTAL			TOTAL	

\* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR			
AMENDMENT	<b>04/04/2011</b>	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 73	Minus ** 73	= 0	X \$26 =	0		X \$ =	
	Independent (37 CFR 1.16(h))	* 7	Minus ***6	= 1	X \$110 =	110		X \$ =	
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR		
					TOTAL ADD'L FEE	<b>110</b>	OR	TOTAL ADD'L FEE	

	(Column 1)	(Column 2)	(Column 3)						
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	X \$ =			X \$ =	
	Independent (37 CFR 1.16(h))	*	Minus ***	=	X \$ =			X \$ =	
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".  
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:  
 /BRUCE HARRISON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/720,147	03/09/2010	Allen F. Rozman	ARAC-01RE1	8473
7590	04/29/2011			
Allen F. Rozman 6402 Wildlife Trail Garland, TX 75044			EXAMINER LAFORGIA, CHRISTIAN A	
			ART UNIT 2439	PAPER NUMBER
			MAIL DATE 04/29/2011	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 12/720,147	<b>Applicant(s)</b> ROZMAN ET AL.	
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1)  Responsive to communication(s) filed on 04 April 2011.
- 2a)  This action is **FINAL**.
- 2b)  This action is non-final.
- 3)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4)  Claim(s) 1-73 is/are pending in the application.
  - 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5)  Claim(s) \_\_\_\_\_ is/are allowed.
- 6)  Claim(s) 1-73 is/are rejected.
- 7)  Claim(s) \_\_\_\_\_ is/are objected to.
- 8)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9)  The specification is objected to by the Examiner.
- 10)  The drawing(s) filed on 09 March 2010 is/are: a)  accepted or b)  objected to by the Examiner.
  - Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
  - Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a)  All    b)  Some \*    c)  None of:
    - 1.  Certified copies of the priority documents have been received.
    - 2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    - 3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1)  Notice of References Cited (PTO-892)
- 2)  Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3)  Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 4/4/11.
- 4)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5)  Notice of Informal Patent Application
- 6)  Other: \_\_\_\_\_.

Art Unit: 2439

### **DETAILED ACTION**

1. The amendment of 04 April 2011 has been noted and made of record.
2. Claims 1-73 have been presented for examination.

### **Information Disclosure Statement**

3. The information disclosure statement (IDS) submitted on 04 April 2011 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement has been considered by the examiner.

### **Response to Arguments**

4. Applicant's arguments, see pages 20-21, filed 04 April 2011, with respect to the rejections made under 35 U.S.C. § 251 have been fully considered and are persuasive. The 35 U.S.C. § 251 rejection of claims 1-57 has been withdrawn.
5. Applicant's arguments, see pages 20-21, filed 04 April 2011, with respect to the rejections made under 35 U.S.C. § 112 have been fully considered and are persuasive. The 35 U.S.C. § 112 rejection of claims 25 and 44-57 has been withdrawn.
6. Applicant's arguments, see pages 20-21, filed 04 April 2011, with respect to the rejections made under 35 U.S.C. § 101 have been fully considered and are persuasive. The 35 U.S.C. § 101 rejection of claims 44-57 has been withdrawn.
7. Applicant's arguments with respect to the prior art rejection of claims 1-57 have been considered but are moot in view of the new grounds of rejection set forth below.

### **Claim Rejections - 35 USC § 102**

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

Art Unit: 2439

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1-4, 5, 7, 10-12, 14-17, 19, 21-26, 29-48, 51-56, 58-67, and 69-73 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent Application Publication No. 2002/0002673 A1 to Narin, hereinafter Narin.

10. As per claim 1, Narin teaches a method of operating a computer system capable of exchanging data across a network of one or more computers and having at least a first and second electronic data processor capable of executing instructions using a common operating system, comprising the steps of:

executing browser instructions in a first logical process within the common operating system using the first electronic data processor, wherein the first logical process is capable of accessing data contained in a first memory space (Figures 2 [element 210, 212], 3 [element 310]), 4 [step 402], paragraphs 0019, 0030, 0031, 0035, 0036, 0040, 0046, i.e. secure application offers a web browsing function in a multiprocessor system);

executing instructions in a second logical process within the common operating system using the second electronic data processor, wherein the second logical process is capable of accessing data contained in the second memory space (Figures 2 [elements 220, 222], 3 [element 320], 4 [step 404], paragraphs 0019, 0032, 0037, 0040-0041, 0050-0051); and

displaying data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to a display (Figures 1 [element 190], 5, Abstract, paragraphs 0007, 0050, 0051, the second process renders its output in a child window of the first process, so that



Art Unit: 2439

the use of a second process to host non-secure software objects is transparent to the user of the first process);

wherein the computer system is configured such that data residing on the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second logical process (Abstract, paragraph 0035-0036, 0039, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

11. Regarding claim 2, Narin teaches wherein the second memory space comprises memory selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figure 2 [element 141], paragraph 0025); a partition on a memory device; random access memory (RAM) (Figure 2 [element 132], paragraph 0023); both volatile and nonvolatile memory.

12. Regarding claim 3, Narin teaches wherein the second logical process comprises a process selected from the group consisting of: an electronic mail process, an instant messaging process, an internet browser process (paragraphs 0007, 0036, 0045-0051), an interactive gaming process, a virtual private network (VPN) process, and a reader application process.

Art Unit: 2439

13. Regarding claim 4, Narin teaches wherein the first logical process receives user interface data and passes the user interface data to the second logical process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042).

14. Regarding claim 5, Narin teaches wherein the first and second electronic data processors are part of a multi-core electronic data processor (paragraph 0019, multi-core electronic data processor is the functional equivalent of a multiprocessor system, neatly packaged in a single-chip).

15. Regarding claim 7, Narin teaches automatically deleting at least one data file residing on the second memory space when the second logical process is terminated (Figure 4 [step 412], paragraph 0044).

16. As per claims 10 and 15, Narin teaches a multiprocessor computer system (Figure 1 [element 120], paragraphs 0019, 0021, multiprocessor systems) using a common operating system capable of exchanging data across a network of one or more computers via a network interface device, comprising:

a first electronic data processor capable of executing browser instructions using the common operating system and communicatively coupled to a first memory space (Figures 2 [element 210, 212], 3 [element 310]], 4 [step 402], paragraphs 0019, 0030, 0031, 0035, 0036, 0040, 0046, i.e. secure application offers a web browsing function in a multiprocessor system);

Art Unit: 2439

a second electronic data processor capable of executing browser instructions using the common operating system and communicatively coupled to a second memory space (Figures 2 [elements 220, 222], 3 [element 320], 4 [step 404], paragraphs 0019, 0032, 0037, 0040-0041, 0050-0051);

a video processor adapted to combine video data from the first and second electronic processors and transmit the combined video data to a display (Figures 1 [element 190], 5, Abstract, paragraphs 0007, 0050, 0051, the second process renders its output in a child window of the first process, so that the use of a second process to host non-secure software objects is transparent to the user of the first process);

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first electronic memory space is protected from corruption by a malware process downloaded from the network and executing on the second electronic data processor (Abstract, paragraph 0035-0036, 0039, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

17. Regarding claim 11, Narin teaches wherein the second memory space comprises memory selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figure 2 [element 141], paragraph 0025); a partition on a memory device; random access memory (RAM) (Figure 2 [element 132], paragraph 0023); both volatile and nonvolatile memory.

Art Unit: 2439

18. Regarding claim 12, Narin teaches wherein the first and second electronic data processors are part of a dual processor computer system (Figure 1 [element 120], paragraphs 0019, 0021, multiprocessor systems).

19. Regarding claims 14 and 16, Narin teaches wherein the computer system is configured such that the first electronic data processor is protected from executing instructions initiated by a malware process downloaded from the network and executing on the second electronic data processor (Abstract, paragraph 0035-0036, 0039, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

20. Regarding claim 17, Narin teaches at least one network interface device capable of exchanging data with the network and with a logical process selected from the group consisting of: the first logical process and the second logical process (paragraph 0036, secure application 312 may provide some type of web-browsing functionality, which would require exchanging data with the network interface device).

21. Regarding claim 19, Narin teaches wherein the at least one electronic data processor comprises a processor selected from the group consisting of: a multi-core electronic data

Art Unit: 2439

processor; dual electronic data processors (Figure 1 [element 120], paragraphs 0019, 0021, multiprocessor systems).

22. As per claim 21, Narin teaches a portable computer capable of executing instructions using a common operating system (paragraph 0019, i.e. handheld or laptop devices), comprising:

a network interface device (Figure 1 [element 170]) configured to exchange data across a network of one or more computers and access at least one website (paragraphs 0026, 0027, 0048, 0049);

at least a first memory space (Figure 2 [elements 132, 141, 212]) and a second memory space (Figure 2 [elements 132, 141, 222]), the first memory space containing at least one system file (Figure 1 [element 134], paragraphs 0030, 0031);

at least one electronic data processor (Figure 1 [element 120]) communicatively coupled (Figure 1 [element 121], system bus) to the network interface device (Figure 1 [element 170]), the first (Figure 2 [elements 132, 141, 212]) and second memory space (Figure 2 [elements 132, 141, 222]), and to a user interface, wherein the user interface is configured to receive input from a computer user (Figure 1 [element 160], paragraph 0025);

the at least one electronic data processor configured to execute a first browser process in a first logical process, wherein the first logical process is capable of accessing data contained in the first memory space (Figures 2 [element 210, 212], 3 [element 310]], 4 [step 402], paragraphs 0030, 0031, 0035, 0036, 0040, 0046, i.e. secure application offers a web browsing function);

the at least one electronic data processor further configured to execute a second browser process in a second logical process within the common operating system (Figures 2 [element

Art Unit: 2439

220], 3 [element 320], 4 [step 404], paragraphs 0032, 0037, 0040), wherein the second logical process is capable of accessing data contained in the second memory space (Figure 2 [elements 220, 222]) and is further capable of generating video data from a website access via the network (Figures 3 [element 322], 4 [steps 406, 410], paragraphs 0040-0041,0050-0051, rendering webpage data, which one of ordinary skill in the art would construe as containing video data, in the non-secure process);

a video processor (Figure 1 [element 190]) configured to transmit video data from the second browser process to a display (Figure 5, Abstract, paragraphs 0007, 0050, 0051, the second process renders its output in a child window of the first process, so that the use of a second process to host non-secure software objects is transparent to the user of the first process);

wherein the first browser process is capable of opening the second browser process and is further capable of passing data to the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application may initiate the hosting of the non-secure software object by instructing the host application to load and execute a non-secure software object within the separate process);

wherein further the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing within the second browser process (Abstract, paragraph 0035-0036, 0039, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

Art Unit: 2439

23. Regarding claim 22, Narin teaches wherein the first browser process is capable of exchanging data with the network interface device (paragraph 0036, secure application 312 may provide some type of web-browsing functionality, which would require exchanging data with the network interface device) and with the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application communicates with hosting application, which hosts non-secure objects).

24. With regards to claim 23, Narin teaches wherein the first browser process is capable of passing data downloaded from the network to the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042).

25. Regarding claim 24, Narin teaches wherein the second browser process is capable of exchanging data with the network interface device (paragraph 0036, non-secure software object is a web browser, which includes the second process exchanging data via the network interface device) and with the first browser process (Figure 5, Abstract, paragraphs 0007, 0050, 0051, the second process communicates with the first process for the purpose of rendering its output in a child window of the first process).

26. Regarding claim 25, Narin teaches wherein the at least one electronic data processor is selected from the group consisting of: an Application Specific Integrated Circuit; a Field Programmable Gate Array; a plurality of electronic data processors (Figure 1 [element 120], paragraphs 0019, 0021, multiprocessor systems); a multi-core electronic data processor.

Art Unit: 2439

27. Regarding claim 26, Narin teaches wherein the second memory space is selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figure 2 [element 141], paragraph 0025); a partition on a memory device; random access memory (RAM) (Figure 2 [element 132], paragraph 0023); both volatile and nonvolatile memory.

28. Regarding claim 29, Narin teaches at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated (Figure 4 [step 412], paragraph 0044).

29. Regarding claim 30, Narin teaches that the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process (Abstract, paragraph 0035-0036, the first process's address space is inaccessible to the second process).

30. Regarding claim 31, Narin teaches wherein attempts by malware to record data entry by the computer user are effectively blocked (paragraph 0035, provide defense against observation and/or modification).

31. As per claim 32, Narin teaches a method of operating a portable computer (paragraph 0019, i.e. handheld or laptop devices) capable of executing instructions using a common



Art Unit: 2439

operating system and having at least one electronic data processor (Figure 1 [element 120]) communicatively coupled (Figure 1 [element 121], system bus) to a first (Figure 2 [elements 132, 141, 212]) and second memory space (Figure 2 [elements 220, 222]) and to a network interface device (Figure 1 [element 170]), comprising:

exchanging data across a network of one or more computers with the network interface device and accessing at least one website (paragraphs 0026, 0027, 0048, 0049);

storing at least one system file within the first memory space (Figures 1 [element 134], 2 [elements 132, 141, 212], paragraphs 0030, 0031);

executing a first browser process in a first logical process within the common operating system using the at least one electronic data processor, wherein the first logical process is configured to access data contained in the first memory space (Figures 2 [element 210, 212], 3 [element 310]), 4 [step 402], paragraphs 0030, 0031, 0035, 0036, 0040, 0046, i.e. secure application offers a web browsing function);

executing a second browser process in a second logical process within the common operating system using the at least one electronic data processor (Figures 2 [element 220], 3 [element 320], 4 [step 404], paragraphs 0032, 0037, 0040), wherein the second logical process is configured to access data contained in the second memory space (Figure 2 [elements 220, 222]) and is further configured to generate video data (Figures 3 [element 322], 4 [steps 406, 410], paragraphs 0040-0041, 0050-0051, rendering webpage data, which one of ordinary skill in the art would construe as containing video data, in the non-secure process);

opening the second browser process on instruction from the first browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure

Art Unit: 2439

application may initiate the hosting of the non-secure software object by instructing the host application to load and execute a non-secure software object within the separate process);

passing data from the first browser process to the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application communicates with hosting application, which hosts non-secure objects);

displaying website video data from the second browser process (Figure 5, Abstract, paragraphs 0007, 0050, 0051, the second process renders its output in a child window of the first process, so that the use of a second process to host non-secure software objects is transparent to the user of the first process);

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process (Abstract, paragraph 0035-0036, 0039, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

32. Regarding claim 33, Narin teaches wherein the portable computer is configured such that the first browser process is capable of exchanging data with the network interface device (paragraph 0036, secure application 312 may provide some type of web-browsing functionality, which would require exchanging data with the network interface device) and with the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application communicates with hosting application, which hosts non-secure objects).

Art Unit: 2439

33. With regards to claim 34, Narin teaches downloading data from the network and passing the data from the first browser process to the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042).

34. Regarding claim 35, Narin teaches wherein the portable computer is configured such that the second browser process is capable of directly exchanging data with the network interface device (paragraph 0036, non-secure software object is a web browser, which includes the second process exchanging data via the network interface device) and with the first browser process (Figure 5, Abstract, paragraphs 0007, 0050, 0051, the second process communicates with the first process for the purpose of rendering its output in a child window of the first process).

35. Regarding claim 36, Narin teaches wherein the second memory space is selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figure 2 [element 141], paragraph 0025); random access memory (RAM) (Figure 2 [element 132], paragraph 0023); both volatile and nonvolatile memory.

36. Regarding claim 39, Narin teaches deleting at least one corrupted data file residing on the second memory space when the second logical process is terminated (Figure 4 [step 412], paragraph 0044).

37. Regarding claim 40, Narin teaches wherein the at least one electronic data processor is

Art Unit: 2439

selected from the group consisting of: an Application Specific Integrated Circuit; a Field Programmable Gate Array; a plurality of electronic data processors (Figure 1 [element 120], paragraphs 0019, 0021, multiprocessor systems); a multi-core electronic data processor.

38. Regarding claim 41, Narin teaches wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process (Abstract, paragraph 0035-0036, the first process's address space is inaccessible to the second process).

39. Regarding claim 42, Narin teaches displaying video data from the first browser process (Figure 5, Abstract, paragraphs 0007, 0050, 0051, the second process renders its output in a child window of the first process, so that the use of a second process to host non-secure software objects is transparent to the user of the first process).

40. Regarding claim 43, Narin teaches wherein attempts by malware to record data entry by the computer user are effectively blocked (paragraph 0035, provide defense against observation and/or modification).

41. As per claims 44 and 64, Narin teaches a method of and non-transitory computer readable medium containing instructions for operating a portable computer (paragraph 0019, i.e. handheld or laptop devices) comprising a network interface device (Figure 1 [element 170]), at least a first memory space (Figure 2 [elements 132, 141, 212]) and a second memory space (Figure 2

Art Unit: 2439

[elements 220, 222]), and at least one electronic data processor communicatively coupled (Figure 1 [element 121], system bus) to the network interface device, the first and second memory space, and to a user interface, comprising:

exchanging data across a network of one or more computers with the network interface device and accessing at least one website (paragraphs 0026, 0027, 0048, 0049);

storing at least one system file in the first memory space (Figures 1 [element 134], 2 [elements 132, 141, 212], paragraphs 0030, 0031);

opening a first browser process, wherein the first browser process is capable of accessing data contained in the first memory space (Figures 2 [element 210, 212], 3 [element 310]), 4 [step 402], paragraphs 0030, 0031, 0035, 0036, 0040, 0046, i.e. secure application offers a web browsing function);

opening a second browser process (Figures 2 [element 220], 3 [element 320], 4 [step 404], paragraphs 0032, 0037, 0040), wherein the second browser process is capable of accessing data contained in the second memory space (Figure 2 [elements 220, 222]), and is further capable of generating data for video display (Figures 3 [element 322], 4 [steps 406, 410], paragraphs 0040-0041, 0050-0051, rendering webpage data, which one of ordinary skill in the art would construe as containing video data, in the non-secure process);

passing data from the first browser process to the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application communicates with hosting application, which hosts non-secure objects);

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from

Art Unit: 2439

the network and executing as part of the second browser process (Abstract, paragraph 0035-0036, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

42. Regarding claim 45, Narin teaches wherein the first browser process is capable of exchanging data with the network interface device (paragraph 0036, secure application 312 may provide some type of web-browsing functionality, which would require exchanging data with the network interface device) and with the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application communicates with hosting application, which hosts non-secure objects).

43. With regards to claim 46, Narin teaches downloading data from the network and passing the downloaded data from the first browser process to the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042).

44. Concerning claim 47, Narin teaches storing the downloaded data on the second memory space (paragraph 0036, non-secure software object runs web-browsing which includes downloading data).

45. Regarding claim 48, Narin teaches wherein the second browser process is capable of exchanging data with the network interface device (paragraph 0036, non-secure software object

Art Unit: 2439

is a web browser, which includes the second process exchanging data via the network interface device) and with the first browser process (Figure 5, Abstract, paragraphs 0007, 0050, 0051, the second process communicates with the first process for the purpose of rendering its output in a child window of the first process).

46. Regarding claim 51, Narin teaches that at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated (Figure 4 [step 412], paragraph 0044).

47. Regarding claim 52, Narin teaches wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process (Abstract, paragraph 0035-0036, 0039, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

48. Regarding claim 53, Narin teaches the first browser process instructing the second browser process to open (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application may initiate the hosting of the non-secure software object by instructing the host application to load and execute a non-secure software object within the separate process).

Art Unit: 2439

49. Regarding claim 54, Narin teaches wherein attempts by malware to record data entry by the computer user are effectively blocked (paragraph 0035, provide defense against observation and/or modification).

50. Regarding claim 55, Narin teaches wherein the at least one electronic data processor comprises a processor selected from the group consisting of: an Application Specific Integrated Circuit; a Field Programmable Gate Array; a plurality of electronic data processors (Figure 1 [element 120], paragraphs 0019, 0021, multiprocessor systems); a multi-core electronic data processor.

51. Regarding claim 56, Narin teaches wherein the second memory space comprises memory selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figure 2 [element 141], paragraph 0025); a partition on a memory device; random access memory (RAM) (Figure 2 [element 132], paragraph 0023); both volatile and nonvolatile memory.

52. Regarding claims 58, 60, 62, and 72, Narin teaches wherein the network interface is capable of exchanging data with the network using a wireless connection (paragraph 0022, wireless media).



Art Unit: 2439

53. With regards to claims 59, 61, 63, and 73, Narin teaches wherein the network comprises a cellular data carrier network (paragraph 0022, cellular networks use RF, or radio frequency).

54. Regarding claim 65, Narin teaches wherein the first browser process is capable of opening the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application may initiate the hosting of the non-secure software object by instructing the host application to load and execute a non-secure software object within the separate process) and the program code stored in the non-transitory computer readable medium is further configured to pass data to the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042).

55. Regarding claim 66, Narin teaches wherein the second logical process is configured to generate data for display and the program code stored in the non-transitory computer readable medium is further configured to process website video data from the second browser process (Figures 3 [element 322], 4 [steps 406, 410], paragraphs 0040-0041, 0050-0051, rendering webpage data, which one of ordinary skill in the art would construe as containing video data, in the non-secure process).

56. Regarding claim 67, Narin teaches wherein the first browser process is capable of directly exchanging data with the network interface device (paragraph 0036, secure application 312 may provide some type of web-browsing functionality, which would require exchanging data with the network interface device) and the second browser process (Figures 3 [elements 326, 238], 4 [step

Art Unit: 2439

408], paragraphs 0037-0038, 0041-0042, secure application communicates with hosting application, which hosts non-secure objects) or the second browser process is capable of directly exchanging data with the network interface device (paragraph 0036, non-secure software object is a web browser, which includes the second process exchanging data via the network interface device) and the first browser process (Figure 5, Abstract, paragraphs 0007, 0050, 0051, the second process communicates with the first process for the purpose of rendering its output in a child window of the first process).

57. Regarding claim 69, Narin teaches wherein at least one corrupted file residing on the second memory space is capable of being deleted when the second browser process is terminated (Figure 4 [step 412], paragraph 0044).

58. Regarding claim 70, Narin teaches wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process (Abstract, paragraph 0035-0036, 0039, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

59. Regarding claim 71, Narin teaches wherein attempts by malware to record data entry by a computer user are effectively blocked (paragraph 0035, provide defense against observation and/or modification).

Art Unit: 2439

**Claim Rejections - 35 USC § 103**

60. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

61. Claims 6, 20, 27, 28, 37, 38, 49, 50, and 68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narin in view of U.S. Patent No. 7,024,581 B1 to Wang et al., hereinafter Wang.

62. Regarding claims 6, 20, 27, 37, 49, and 68, Narin does not teach at least one corrupted file required for a browser process is capable of being restored from a protected image.

63. Wang teaches restoring at least one corrupted data file from a protected image (Figures 2 [elements 72, 74, 76, 78, 80, 82], 3 [element 140], 6 [element 236], 7 [element 272], column 9, lines 13-67).

64. It would have been obvious to one of ordinary skill in the art at the time the invention was made to restore at least one corrupted data file from a protected image, since Wang states at column 2, lines 49-60 that using a protected image takes advantage of today's computing power and storage capabilities to increase the reliability, accessibility, flexibility, and performance of computers and the backup/restore process.

65. With regards to claims 28, 38, and 50, Wang teaches wherein the protected image is stored at a location selected from the group consisting of: a removable drive; the first memory space; a partition on a memory device image (Figures 2 [elements 72, 74, 76, 78, 80, 82], 3

Art Unit: 2439

[element 140], 6 [element 236], 7 [element 272], column 9, lines 13-67); a nonvolatile memory disk; another device (Figure 4).

66. Claim 57 is rejected under 35 U.S.C. 103(a) as being unpatentable over Narin.

67. Regarding claim 57, Narin does not teach the first browser process opening a plurality of second browser processes.

68. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the first browser process to open a plurality of second browser processes, since one of ordinary skill in the art would recognize that web pages may have several processes from different service providers that could be regarded as nefarious, thereby having a need to generate a second process for each of the potentially nefarious processes. Furthermore, it has been held that merely duplicating a part or its function has no patentable significance unless it produces new and unexpected results. See MPEP § 2144.04(VI)(B).

### **Double Patenting**

69. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re*

Art Unit: 2439

Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

70. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

71. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

72. Claims 21-73 are provisionally rejected on the ground of nonstatutory double patenting over claims 21-55 of copending Application No. 12/720,207. This is a provisional double patenting rejection since the conflicting claims have not yet been patented.

73. The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on that copending application since the referenced copending application and the instant application are claiming common subject matter, and only differ in the type of device implementing the claimed invention.

#### **Allowable Subject Matter**

74. Claims 8, 9, 13, and 18 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base

Art Unit: 2439

claim and any intervening claims. Claims 8, 9, 13, and 18 would be allowable if the rejections set forth in this Office action were overcome and all of the limitations of the base claim and any intervening claims were included in those claims.

### **Conclusion**

75. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

76. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

77. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/  
Primary Examiner, Art Unit 2439

clf

<b>Notice of References Cited</b>	Application/Control No. 12/720,147	Applicant(s)/Patent Under Reexamination ROZMAN ET AL.	
	Examiner Christian LaForgia	Art Unit 2439	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-2002/0002673 A1	01-2002	Narin, Attila	713/152
*	B US-2004/0006706 A1	01-2004	Erlingsson, Ulfar	713/200
*	C US-2004/0267929 A1	12-2004	Xie, Michael	709/225
*	D US-2005/0149726 A1	07-2005	Joshi et al.	713/164
*	E US-7,039,801 B2	05-2006	Narin, Attila	713/152
*	F US-7,650,493 B2	01-2010	Narin, Attila	713/152
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			

**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

**NON-PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	36	rozman-all\$.in.	US-PGPUB; USPAT	OR	OFF	2007/09/13 09:28
S2	2	cioffi-alf\$.in.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:49
S3	1	"6289462".pn.	US-PGPUB; USPAT	OR	OFF	2007/09/13 09:32
S4	10	((("7146640") or ("5835695") or ("6578140") or ("20050149933") or ("6892261") or ("6678712") or ("6957286") or ("6996828") or ("20040205755") or ("6697972")).PN.	US-PGPUB; USPAT	OR	OFF	2007/09/13 09:33
S5	5	("6578140").URPN.	USPAT	OR	OFF	2007/09/13 10:01
S6	1	(dual multiple) near (OS operat\$3 near systems) with (prevent\$3 stop\$4) with (virus trojan malicious malware)	US-PGPUB; USPAT	OR	ON	2007/09/13 10:06
S7	15	("6385721").URPN.	USPAT	OR	OFF	2007/09/13 10:03
S8	8	(dual multiple) near (OS operat\$3 near systems) with (virus trojan malicious malware)	US-PGPUB; USPAT	OR	ON	2007/09/13 13:58
S9	0	("2004/0039944").URPN.	USPAT	OR	OFF	2007/09/13 10:09
S10	35	((("5826013") or ("5978917") or ("6735700") or ("6663000") or ("6553377") or ("6216112") or ("4890098") or ("5555364") or ("5666030") or ("5995103") or ("5502808") or ("5280579") or ("5918039") or ("6480198") or	US-PGPUB; USPAT	OR	OFF	2007/09/13 10:13



		("6167522") or ("6199181") or ("6275938") or ("6351816") or ("6456554") or ("6658573") or ("6507904") or ("6633963") or ("6678825") or ("5751979") or ("20040054588") or ("20040034794") or ("20040006715") or ("20030177397") or ("20030097591") or ("20030023857") or ("20020066016") or ("20020174349") or ("6581162") or ("6134661") or ("6578140").PN.				
S11	8	(US-20040039944-\$).did. or (US-7146640-\$ or US- 6996828-\$ or US-6678712- \$ or US-6578140-\$ or US- 6385721-\$ or US-7260839- \$ or US-6199181-\$).did.	US-PGPUB; USPAT	OR	OFF	2007/09/13 10:28
S12	0	S11 and network\$3 near (OS operat\$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 10:29
S13	8565	network\$3 near (OS operat \$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 10:29
S14	2	(dual multiple) near (OS operat\$3 near systems) same (display\$3) with both with (OS\$2 operat\$3 near systems)	US-PGPUB; USPAT	OR	ON	2007/09/13 11:55
S15	67	(dual multiple) near (OS operat\$3 near systems) same (display\$3) with (multiple) with (OS\$2 operat\$3 near systems)	US-PGPUB; USPAT	OR	ON	2007/09/13 11:55
S16	41	("5673403").URPN.	USPAT	OR	OFF	2007/09/13 12:12
S17	4565	(dual multiple) near (OS operat\$3 near systems)	US-PGPUB; USPAT	OR	ON	2007/09/13 14:49
S18	688	multi\$score near (processor cpu)	US-PGPUB; USPAT	OR	ON	2007/09/13 13:59
S19	37	S17 and S18	US-PGPUB; USPAT	OR	ON	2007/09/13 13:59
S20	18	S17 same S18	US-PGPUB; USPAT	OR	ON	2007/09/13 14:00

S21	4	S17 with S18	US-PGPUB; USPAT	OR	ON	2007/09/13 13:59
S22	14	S17 same S18 not S21	US-PGPUB; USPAT	OR	ON	2007/09/13 14:01
S23	19	S19 not S20	US-PGPUB; USPAT	OR	ON	2007/09/13 14:01
S24	665	(dual multiple) near (OS operat\$3 near systems) and (remov\$3 delet\$3) with (file program)	US-PGPUB; USPAT	OR	ON	2007/09/13 14:50
S25	1	(dual multiple) near (OS operat\$3 near systems) and (remov\$3 delet\$3) with (file program) with after near (run\$3 ran execut\$3)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:09
S26	17	(dual multiple) near (OS operat\$3 near systems) with encrypt\$3 \	US-PGPUB; USPAT	OR	ON	2007/09/13 15:09
S27	17	(dual multiple) near (OS operat\$3 near systems) with encrypt\$3	US-PGPUB; USPAT	OR	ON	2007/09/13 15:19
S28	36	(dual multiple) near (OS operat\$3 near systems) same encrypt\$3	US-PGPUB; USPAT	OR	ON	2007/09/13 15:19
S29	19	(dual multiple) near (OS operat\$3 near systems) same encrypt\$3 not S27	US-PGPUB; USPAT	OR	ON	2007/09/13 15:23
S30	676	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 not S28	US-PGPUB; USPAT	OR	ON	2007/09/13 15:33
S31	12	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (inter \$OS inter\$operat\$3 near system inter\$process\$2)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:35
S32	0	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (data information) with first near (OS operat\$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:38
S33	1	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with first near (OS operat\$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:37

S34	9	(US-20040039944-\$).did. or (US-7146640-\$ or US- 6996828-\$ or US-6678712- \$ or US-6578140-\$ or US- 6385721-\$ or US-7260839- \$ or US-6199181-\$ or US- 5673403-\$).did.	US-PGPUB; USPAT	OR	OFF	2007/09/13 15:37
S35	2	S34 and encrypt\$3	US-PGPUB; USPAT	OR	ON	2007/09/13 15:37
S36	81	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (OS operat\$3 near system) with (transfer communicat\$3 data)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:39
S37	6	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (OS operat\$3 near system) with (transfer communicat\$3)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:39
S38	0	731/1.ccls.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:12
S39	2670	713/1.ccls.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:12
S40	1	"7027872".pn.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:52
S41	0	"7027872".pn. and IMD with (authentikat\$3 authori \$6 verif\$7 valid\$5)	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:52
S42	1	"7027872".pn. and (authentikat\$3 authori\$6 verif\$7 valid\$5)	US-PGPUB; USPAT	OR	OFF	2007/09/13 17:06
S43	1	"20050022020".pn.	US-PGPUB; USPAT	OR	OFF	2007/09/13 17:06
S44	1	"6192477".pn.	US-PGPUB; USPAT	OR	OFF	2008/02/19 13:13
S45	9	("6192477").URPN.	USPAT	OR	OFF	2008/02/19 13:14
S46	9	("6192477").URPN.	USPAT	OR	OFF	2008/06/16 16:15
S47	9	("6192477").URPN.	USPAT	OR	OFF	2008/06/16 16:15
S48	5	("6578140").URPN.	USPAT	OR	OFF	2008/08/18 14:31
S49	63	secure near3 process\$3 same insecure near3 process\$3	US-PGPUB; USPAT	OR	ON	2008/08/18 14:32

S50	1	secure near3 process\$3 same insecure near3 process\$3 with (internet e \$1mail)	US-PGPUB; USPAT	OR	ON	2008/08/18 14:32
S51	0	secure near3 processor and insecure near3 processor with (internet e \$1mail)	US-PGPUB; USPAT	OR	ON	2008/08/18 14:33
S52	9	("6192477").URPN.	USPAT	OR	OFF	2008/08/18 16:04
S53	1	common near (operat\$3 nears system OS) same protect\$3 near processor	US-PGPUB; USPAT	OR	ON	2008/08/18 16:33
S54	36	common near (operat\$3 nears system OS) and protect\$3 near processor	US-PGPUB; USPAT	OR	ON	2008/08/18 16:33
S55	0	(common near (operat\$3 nears system OS) and protect\$3 near processor). clm.	US-PGPUB; USPAT	OR	ON	2008/08/18 16:34
S56	1	"7484247".pn.	US-PGPUB; USPAT	OR	OFF	2010/12/21 13:22
S57	8	((("5673403") or ("5751979") or ("5974549") or ("5978917") or ("6091412") or ("6134661") or ("6397242") or ("6401134")).PN.	USPAT	OR	OFF	2010/12/21 13:27
S58	173	("5974549").URPN.	USPAT	OR	OFF	2010/12/21 13:29
S59	11	((("6433794") or ("6438600") or ("6492995") or ("6678825") or ("6691230") or ("6757685") or ("6836885") or ("7024555") or ("7139890") or ("7146640") or ("7260839")).PN.	USPAT	OR	OFF	2010/12/21 13:48
S60	3	((("7401230") or ("7421689") or ("7565522")).PN.	USPAT	OR	OFF	2010/12/21 13:51
S61	1291	eros	US-PGPUB; USPAT	OR	ON	2010/12/21 14:13
S62	12	eros and ("726" "713" "380").clas.	US-PGPUB; USPAT	OR	ON	2010/12/21 14:13

S63	0	eros with trust\$3 with window	US-PGPUB; USPAT	OR	ON	2010/12/21 14:14
S64	8	((("4890098") or ("5280579") or ("5502808") or ("5555364") or ("5666030") or ("5673403") or ("5751979") or ("5826013"))).PN.	USPAT	OR	OFF	2010/12/21 14:54
S65	11	((("5918039") or ("5978917") or ("5995103") or ("6134661") or ("6167522") or ("6192477") or ("6199181") or ("6216112") or ("6275938") or ("6351816") or ("6385721"))).PN.	USPAT	OR	OFF	2010/12/21 14:56
S66	11	((("6480198") or ("6507904") or ("6507948") or ("6546554") or ("6553377") or ("6578140") or ("6581162") or ("6633963") or ("6658573") or ("6663000") or ("6678825"))).PN.	USPAT	OR	OFF	2010/12/21 14:58
S67	65	("6678825").URPN.	USPAT	OR	OFF	2010/12/21 14:58
S68	8	("6578140").URPN.	USPAT	OR	OFF	2010/12/21 15:09
S69	4	((("6735700") or ("6321337") or ("7146640") or ("7260839"))).PN.	USPAT	OR	OFF	2010/12/21 15:10
S70	5	((("20020066016") or ("20020174349") or ("20030023857") or ("20030097591") or ("20030177397"))).PN.	US-PGPUB	OR	OFF	2010/12/21 15:12
S71	6	((("20040006715") or ("20040034794") or ("20040039944") or ("20040054588") or ("20050240810") or ("20060004667"))).PN.	US-PGPUB	OR	OFF	2010/12/21 15:13

S72	8	(("6880110") or ("7096381") or ("7577871") or ("7694328") or ("7373505") or ("7039801") or ("7596694") or ("7085928")).PN.	USPAT	OR	OFF	2010/12/21 15:18
S73	11	(("7181768") or ("7284274") or ("6804780") or ("7191469") or ("6505300") or ("7246374") or ("7062672") or ("7444412") or ("6772345") or ("6108715") or ("6873988")).PN.	USPAT	OR	OFF	2010/12/21 15:21
S74	1	"20030131152".pn.	US-PGPUB; USPAT	OR	OFF	2010/12/21 15:23
S75	4522	janus	US-PGPUB; USPAT	OR	OFF	2010/12/21 15:24
S76	1	"7484247".pn.	US-PGPUB; USPAT	OR	OFF	2010/12/21 15:47
S77	0	("7818808").URPN.	USPAT	OR	OFF	2010/12/22 06:08
S78	38	(execut\$3 run\$4) with (web HTML XML content) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:10
S79	2	(execut\$3 run\$4) with (plug \$in applet java\$script embed\$4 near executable) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:15
S80	2	(execut\$3 run\$4 render\$3) with (plug\$in applet java \$script embed\$4 near executable) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:15
S81	4	(execut\$3 run\$4 render\$3) with (malicious virus malware trojan spyware adware) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:17
S82	3	("2005/0005153").URPN.	USPAT	OR	OFF	2010/12/22 06:20

S83	2	(execut\$3 run\$4) with (plug \$in applet java\$script embed\$4 near (content executable)) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:21
S84	0	(execut\$3 run\$4 render\$3) with (separate isolat\$3) near (CPU processor microprocessor) same (detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:21
S85	70	(execut\$3 run\$4 render\$3) with (separate isolat\$3) near (CPU processor microprocessor) and (detect \$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:21
S86	35	sandbox\$3 with (CPU processor microprocessor) same (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:29
S87	15	sandbox\$3 with (CPU processor microprocessor) and (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) not S86	US-PGPUB; USPAT	OR	ON	2010/12/22 06:30
S88	9	("20050283836" "20030051027" "20060259948" "20060191008" "20060080735" "6785732" "20050131868" "20010032205" "20060101514").pn.	US-PGPUB; USPAT	OR	ON	2010/12/22 06:33
S89	4	(web internet embed\$4) near (video audio content media) with (CPU processor microprocessor) same (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:37
S90	54	("5751979").URPN.	USPAT	OR	OFF	2010/12/22 06:39

S91	67	(web internet embed\$4) near (video audio content media) with (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:41
S92	3	(separate isolat\$3) near (CPU processor microprocessor) with (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:47
S93	5	(execut\$3 run\$4 render\$3) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:56
S94	0	((web internet embed\$4) near (content media video audio page site) web\$site web\$page) with (separate isolat\$3) near (CPU processor microprocessor) same (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:57
S95	3	(separate isolat\$3) near (CPU processor microprocessor) with (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:57
S96	1181	(CPU processor microprocessor) with (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:58



S97	15	(CPU processor microprocessor) with (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware) with ((web internet embed\$4) near (content media video audio page site) web\$site web \$page)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:58
S98	15	(CPU processor microprocessor) with (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware) with ((web internet embed\$4) near (content media video audio page site) web\$site web \$page) not S87	US-PGPUB; USPAT	OR	ON	2010/12/22 06:59
S99	0	(separate special\$4 isolat \$3 individual\$4) with (CPU processor microprocessor) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin \$5 check\$3) with (malicious virus malware trojan spyware adware) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page) not S87	US-PGPUB; USPAT	OR	ON	2010/12/22 07:03
S100	0	(separate special\$4 isolat \$3 individual\$4) with (CPU processor microprocessor) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page) same (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3 prevent\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:03

S101	31	(CPU processor microprocessor) with ((web internet embed\$4) near (content media video audio page site) web\$site web \$page) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3 prevent\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:04
S102	0	(execut\$3 run\$4 render\$3) with (separate isolat\$3) near (CPU processor microprocessor) with sandbox\$3	US-PGPUB; USPAT	OR	ON	2010/12/22 07:11
S103	0	(separate isolat\$3) near (CPU processor microprocessor) with sandbox\$3	US-PGPUB; USPAT	OR	ON	2010/12/22 07:11
S104	36	(CPU processor microprocessor) with sandbox\$3 with (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3 prevent\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:11
S105	11	(("20050198692") or ("20050234856") or ("20060242166") or ("20060242709") or ("20060271835") or ("20080184105") or ("20080178302") or ("20080263358") or ("7562293") or ("7607172") or ("7698559")).PN.	US-PGPUB; USPAT	OR	OFF	2010/12/22 07:14
S106	2	("2005/0198692").URPN.	USPAT	OR	OFF	2010/12/22 07:21
S107	8	("20050198692"   "5832208"   "6092194"   "6240530"   "6675174"   "6701440"   "7171691"   "7263561").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2010/12/22 07:22
S108	54	("5751979").URPN.	USPAT	OR	OFF	2010/12/22 07:24

S109	0	(divid\$3 division split\$4 spread\$3) with (CPU processor microprocessor) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page) same (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:41
S110	7	(divid\$3 division split\$4 spread\$3) with (CPU processor microprocessor) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page) and (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:42
S111	183	(divid\$3 division split\$4 spread\$3) with (CPU processor microprocessor) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:43
S112	61	(execut\$3 run\$4 render\$3 display\$3 reproduc\$3) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page plug\$in script java\$script perl\$script) with (separate isolat\$3 individual second other) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 11:02
S113	9	(execut\$3 run\$4 render\$3 display\$3 reproduc\$3) with (suspicious malicious malware suspect\$2) with (separate isolat\$3 individual second other) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 14:18

S114	68	(execut\$3 run\$4 render\$3 display\$3 reproduc\$3) with (download\$2) with (separate isolat\$3 individual second other) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 14:20
S115	178	("5974549").URPN.	USPAT	OR	OFF	2010/12/28 14:11
S116	1	(CPU processor micro \$processor) with delegat\$3 same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin \$5 check\$3) with (malicious virus malware trojan spyware adware)	USPAT	OR	ON	2010/12/28 14:16
S117	7	(CPU processor micro \$processor) with delegat\$3 and (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware)	USPAT	OR	ON	2010/12/28 14:17
S118	8	(CPU processor micro \$processor) with (transfer \$4 delegat\$3 assign\$4) with (task process application) same (protect \$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	USPAT	OR	ON	2010/12/28 14:18
S119	19	("6678712").URPN.	USPAT	OR	OFF	2010/12/28 14:21
S120	8	("6578140").URPN.	USPAT	OR	OFF	2010/12/28 14:27
S121	5	("20060107055"   "20080301670"   "6016546"   "6195587"   "6578140").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2010/12/28 14:27
S122	56	(virus anti\$virus) near (processor co\$processor)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:31

S123	3738	(CPU processor micro \$processor co\$processor video adj processor) with (display\$3 render\$3 reproduc\$4) with ((web internet embed\$4) near (content media video audio page site) web\$site web \$page)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:34
S124	1	(CPU processor micro \$processor co\$processor video adj processor) with (display\$3 render\$3 reproduc\$4) with ((web internet embed\$4) near (content media video audio page site) web\$site web \$page) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:35
S125	14	(CPU processor micro \$processor co\$processor video adj processor) with (display\$3 render\$3 reproduc\$4) with ((web internet embed\$4) near (content media video audio page site) web\$site web \$page) and (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:35
S126	95	("6199181").URPN.	USPAT	OR	OFF	2010/12/28 14:38
S127	2	("2004/0039944").URPN.	USPAT	OR	OFF	2010/12/28 14:47
S128	14	("6192477").URPN.	USPAT	OR	OFF	2010/12/28 14:48
S129	1	"7146305".pn.	USPAT	OR	OFF	2010/12/28 14:50

SI30	235	("20010034847"   "20020032717"   "20020032793"   "20020032880"   "20020035698"   "20020083331"   "20020083334"   "20020138753"   "20020144156"   "20030037136"   "20030088791"   "20030212903"   "20040010718"   "4223380"   "4400769"   "4672609"   "4773028"   "4819234"   "4975950"   "5032979"   "5121345"   "5204966"   "5210704"   "5274824"   "5278901"   "5309562"   "5311593"   "5345595"   "5347450"   "5353393"   "5359659"   "5371852"   "5398196"   "5414833"   "5440723"   "5452442"   "5454074"   "5475839"   "5511184"   "5515508"   "5522026"   "5539659"   "5557742"   "5586260"   "5590331"   "5606668"   "5623600"   "5623601"   "5630061"   "5649095"   "5649185"   "5675711"   "5696486"   "5696822"   "5706210"   "5734697"   "5745692"   "5748098"   "5761504"   "5764887"   "5764890"   "5765030"   "5774727"   "5787177"   "5790799"   "5796942"   "5798706"   "5812763"   "5815574"   "5822517"   "5826013"   "5828833"   "5832208"   "5832211"   "5835726"   "5838903"   "5842002"   "5845067"   "5848233"   "5854916"   "5857191"   "5864665"   "5864803"   "5872978"   "5875296"   "5878420"   "5881236"   "5884033"   "5892903"   "5899999"   "5907834"   "5919257"   "5919258"   "5922051"   "5925126"   "5931946"   "5940591"   "5950012"   "5961644"	US-PGPUB; USPAT; USOCR	OR	OFF	2010/12/28 14:50
------	-----	---	------------------------------	----	-----	---------------------

"5964839"	"5964889"
"5974237"	"5974457"
"5978917"	"5983270"
"5983348"	"5983350"
"5987606"	"5987610"
"5987611"	"5991856"
"5991881"	"5999711"
"5999723"	"6003132"
"6006016"	"6009467"
"6014645"	"6016553"
"6021510")	PN. OR
("6026442"	"6029256"
"6035323"	"6035423"
"6041347"	"6052709"
"6061795"	"6067410"
"6070190"	"6070244"
"6073172"	"6081894"
"6085224"	"6088803"
"6088804"	"6092194"
"6094731"	"6098173"
"6104783"	"6108799"
"6118940"	"6119165"
"6119234"	"6122738"
"6144961"	"6154844"
"6161109"	"6167520"
"6173413"	"6185689"
"6195687"	"6199181"
"6205552"	"6226372"
"6230288"	"6266773"
"6266774"	"6271840"
"6272641"	"6275938"
"6275942"	"6278886"
"6279113"	"6282546"
"6298445"	"6301668"
"6314520"	"6314525"
"6321338"	"6324627"
"6324647"	"6324656"
"6338141"	"6347374"
"6353385"	"6357008"
"6377994"	"6396845"
"6397242"	"6397245"
"6405318"	"6405364"
"6408391"	"6415321"
"6429952"	"6434615"
"6438600"	"6445822"
"6453345"	"6453346"
"6460141"	"6463426"
"6470449"	"6477585"
"6477648"	"6477651"
"6484203"	"6487666"
"6496858"	"6499107"
"6510523"	"6517587"
"6519647"	"6519703"
"6530024"	"6535227"
"6546493"	"6563959"
"6574737"	"6578147"
"6584454"	"6601190"

		"6606744"   "6618501"   "6628824"   "6647139"   "6647400"   "6661904"   "6668082"   "6668084"   "6681331"   "6691232"   "6704874"   "6708212"   "6711127"   "6711615"   "6718383"   "6721806"   "6725377"   "6725378"   "6775780"   "6792144"   "6792546"   "6816973"   "6839850"   "6851057"). PN.				
S131	12	("7146305").URPN.	USPAT	OR	OFF	2010/12/28 14:51
S132	5	restor\$3 with (file application program) with protect\$3 near image	US-PGPUB; USPAT	OR	ON	2010/12/28 17:07
S133	49	sub\$operat\$3 near system	US-PGPUB; USPAT	OR	ON	2010/12/29 15:43
S134	4503	(secure protect\$3 sand\$box \$3) with (web internet) near (browser viewer application)	US-PGPUB; USPAT	OR	ON	2010/12/30 11:06
S135	4100	(secure protect\$3 sand\$box \$3) with (web internet) adj (browser viewer application)	US-PGPUB; USPAT	OR	ON	2010/12/30 11:06
S136	4073	(secure protect\$3) with (web internet) adj (browser viewer application)	US-PGPUB; USPAT	OR	ON	2010/12/30 11:07
S137	15	(secure protect\$3) with (web internet) adj (browser viewer application) same sand\$box \$3 with (content media video audio embed\$4)	US-PGPUB; USPAT	OR	ON	2010/12/30 11:07
S138	19	(secure protect\$3) with (web internet) adj (browser viewer application) and sand\$box \$3 with (content media video audio embed\$4) not S137	US-PGPUB; USPAT	OR	ON	2010/12/30 11:09
S139	1	(US-20050149726-\$.)did.	US-PGPUB	OR	OFF	2010/12/30 11:30
S140	1	S139 and scan\$4	US-PGPUB; USPAT	OR	ON	2010/12/30 11:30
S141	55	("2005/0149726").URPN.	USPAT	OR	OFF	2010/12/30 11:33



S142	0	S139 and (permission permitting permit)	USPAT	OR	ON	2010/12/30 11:40
S143	2	(US-20050149726-\$).did. or (US-7146305-\$).did.	US-PGPUB; USPAT	OR	OFF	2010/12/30 12:18
S144	2	S143 and (cell\$4 mobile)	US-PGPUB; USPAT	OR	ON	2010/12/30 12:19
S145	258	list\$3 with block\$3 with (web\$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/30 12:24
S146	2	list\$3 with block\$3 with (web\$site web\$page) with (virus malware infection malicious trojan worm)	US-PGPUB; USPAT	OR	ON	2010/12/30 12:24
S147	4	list\$3 with block\$3 with (web\$site web\$page) same (virus malware infection malicious trojan worm)	US-PGPUB; USPAT	OR	ON	2010/12/30 12:25
S148	3	list\$3 with block\$3 with (web\$site web\$page) and 726/22-24.ccls.	US-PGPUB; USPAT	OR	ON	2010/12/30 12:25
S149	19	list\$3 with block\$3 with (web\$site web\$page) and "726".clas.	US-PGPUB; USPAT	OR	ON	2010/12/30 12:26
S150	10	(list\$3 with block\$3 black \$list\$3) with (web\$site web \$page) with (virus malware infection malicious trojan worm)	US-PGPUB; USPAT	OR	ON	2010/12/30 12:27
S151	16	(list\$3 with block\$3 black \$list\$3) with (web\$site web \$page) same (virus malware infection malicious trojan worm)	US-PGPUB; USPAT	OR	ON	2010/12/30 12:27
S152	6	(list\$3 with block\$3 black \$list\$3) with (web\$site web \$page) same (virus malware infection malicious trojan worm) not S150	US-PGPUB; USPAT	OR	ON	2010/12/30 12:27
S153	10	(list\$3 with block\$3 black \$list\$3) with (web\$site web \$page) and 726/22-24.ccls.	US-PGPUB; USPAT	OR	ON	2010/12/30 12:29
S154	7	(list\$3 with block\$3 black \$list\$3) with (web\$site web \$page) and 726/22-24.ccls. not S150	US-PGPUB; USPAT	OR	ON	2010/12/30 12:29
S155	10	(list\$3 with block\$3 black \$list\$3) with (web\$site web \$page) with (virus malware infect\$3 malicious trojan worm)	US-PGPUB; USPAT	OR	ON	2010/12/30 12:29

S156	43	(list\$3 with block\$3 black \$list\$3) with (web\$site web \$page) and ("726" "713"). clas.	US-PGPUB; USPAT	OR	ON	2010/12/30 12:30
S157	34	(list\$3 with block\$3 black \$list\$3) with (web\$page web\$site site page) with (malicious malware infect \$3 virus) and ("726" "713"). clas.	US-PGPUB; USPAT	OR	ON	2010/12/30 12:32
S158	37	((list\$3 table data\$base) with block\$3 black\$list\$3) with (web\$page web\$site site page) with (malicious malware infect\$3 virus) and ("726" "713").clas.	US-PGPUB; USPAT	OR	ON	2010/12/30 12:34
S159	3	((list\$3 table data\$base) with block\$3 black\$list\$3) with (web\$page web\$site site page) with (malicious malware infect\$3 virus) and ("726" "713").clas. not S157	US-PGPUB; USPAT	OR	ON	2010/12/30 12:34
S160	1	(US-7484247-\$).did.	USPAT	OR	OFF	2010/12/30 15:05
S161	1	"20040267929".pn.	US-PGPUB; USPAT	OR	OFF	2010/12/30 15:06
S162	1	(US-7484247-\$).did. and search\$3 near request\$3	USPAT	OR	ON	2010/12/30 15:06
S163	0	(secure protect\$3) with (web internet) adj (browser viewer application) same (prevent \$3 stop\$4) with search\$3 with (hack malicious\$2 hi \$jack)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:15
S164	1	(secure protect\$3) with (web internet) adj (browser viewer application) and (prevent \$3 stop\$4) with search\$3 with (hack malicious\$2 hi \$jack)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:15
S165	36	(prevent\$3 stop\$4) with search\$3 with (hack malicious\$2 hi\$jack)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:16
S166	58	search\$3 near (engine request) near4 (hack malicious\$2 hi\$jack)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:18
S167	59	search\$3 near (engine request) near4 (hack malicious\$2 hi\$jack\$3)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:19

S168	1	search\$3 near (engine request) near4 (hack malicious\$2 hi\$jack\$3) not S166	US-PGPUB; USPAT	OR	ON	2010/12/30 15:19
S169	3728010	prevent\$3 search\$3 near4 (hack malicious\$2 hi\$jack \$3)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:21
S170	15	prevent\$3 with search\$3 near4 (hack malicious\$2 hi \$jack\$3)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:21
S171	59	("2005/0149726").URPN.	USPAT	OR	OFF	2011/03/03 16:07
S172	59	("2005/0149726").URPN.	USPAT	OR	OFF	2011/03/03 16:07
S173	2915	726/23-24.ccls.	US-PGPUB; USPAT	OR	OFF	2011/04/12 12:48
S174	5374	709/225.ccls.	US-PGPUB; USPAT	OR	OFF	2011/04/12 12:48
S175	93	S173 and S174	US-PGPUB; USPAT	OR	OFF	2011/04/12 12:48
S176	2	S173 and S174 and secure with browser	US-PGPUB; USPAT	OR	ON	2011/04/12 12:49
S177	911	713/151.ccls.	US-PGPUB; USPAT	OR	ON	2011/04/12 12:50
S178	422	713/152.ccls.	US-PGPUB; USPAT	OR	ON	2011/04/12 12:50
S179	25	S178 and S173	US-PGPUB; USPAT	OR	ON	2011/04/12 12:50
S180	1	"7039801".pn.	US-PGPUB; USPAT	OR	OFF	2011/04/12 12:59
S181	4	("7039801").URPN.	USPAT	OR	OFF	2011/04/12 13:38
S182	1	"20020002673".pn.	US-PGPUB; USPAT	OR	OFF	2011/04/12 13:38
S183	5	("6049838"   "6108715"   "6330670"   "6434679"   "6487665").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2011/04/12 13:39
S184	10	("2002/0002673").URPN.	USPAT	OR	OFF	2011/04/12 13:40
S185	0	(block\$3 with modif\$7 with search near request\$3). clm.	US-PGPUB; USPAT	OR	ON	2011/04/12 13:51

### EAST Search History (I nterference)


Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp

S186	0	(block\$3 with modif\$7 with search near request \$3).cm.	USPAT; UPAD	OR	ON	2011/04/12 13:51
------	---	---	-------------	----	----	------------------

**4/ 26/ 11 9:27:35 AM**

**C:\ Documents and Settings\ claforgia\ My Documents\ EAST\ Workspaces\ 12720147.wsp**



<b>Index of Claims</b>  	<b>Application/Control No.</b> 12720147	<b>Applicant(s)/Patent Under Reexamination</b> ROZMAN ET AL.
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/29/2010	04/25/2011						
	1	✓	✓						
	2	✓	✓						
	3	✓	✓						
	4	✓	✓						
	5	✓	✓						
	6	✓	✓						
	7	✓	✓						
	8	✓	✓						
	9	✓	✓						
	10	✓	✓						
	11	✓	✓						
	12	✓	✓						
	13	✓	✓						
	14	✓	✓						
	15	✓	✓						
	16	✓	✓						
	17	✓	✓						
	18	✓	✓						
	19	✓	✓						
	20	✓	✓						
	21	✓	✓						
	22	✓	✓						
	23	✓	✓						
	24	✓	✓						
	25	✓	✓						
	26	✓	✓						
	27	✓	✓						
	28	✓	✓						
	29	✓	✓						
	30	✓	✓						
	31	✓	✓						
	32	✓	✓						
	33	✓	✓						
	34	✓	✓						
	35	✓	✓						
	36	✓	✓						

<b>Index of Claims</b>  	<b>Application/Control No.</b> 12720147	<b>Applicant(s)/Patent Under Reexamination</b> ROZMAN ET AL.
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/29/2010	04/25/2011						
	37	✓	✓						
	38	✓	✓						
	39	✓	✓						
	40	✓	✓						
	41	✓	✓						
	42	✓	✓						
	43	✓	✓						
	44	✓	✓						
	45	✓	✓						
	46	✓	✓						
	47	✓	✓						
	48	✓	✓						
	49	✓	✓						
	50	✓	✓						
	51	✓	✓						
	52	✓	✓						
	53	✓	✓						
	54	✓	✓						
	55	✓	✓						
	56	✓	✓						
	57	✓	✓						
	58		✓						
	59		✓						
	60		✓						
	61		✓						
	62		✓						
	63		✓						
	64		✓						
	65		✓						
	66		✓						
	67		✓						
	68		✓						
	69		✓						
	70		✓						
	71		✓						
	72		✓						

<b><i>Index of Claims</i></b>  	<b>Application/Control No.</b> 12720147	<b>Applicant(s)/Patent Under Reexamination</b> ROZMAN ET AL.
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>


N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/29/2010	04/25/2011						
	73		✓						



<b>Search Notes</b>  	<b>Application/Control No.</b>  12720147	<b>Applicant(s)/Patent Under Reexamination</b>  ROZMAN ET AL.
	<b>Examiner</b>  Christian LaForgia	<b>Art Unit</b>  2439

SEARCHED			
Class	Subclass	Date	Examiner
none	none	12/29/10	clf
726	23-24	4/25/11	clf
713	152	4/25/11	clf
709	225	4/25/11	clf

SEARCH NOTES		
Search Notes	Date	Examiner
updated search for 10/913,609 (USPN 7,484,247)	12/29/10	clf
updated EAST - see enclosed	4/25/11	clf

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

	/Christian LaForgia/ Primary Examiner.Art Unit 2439
--	--

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS</b>	<b>Application Number</b>	12/720,147
	<b>Filing Date</b>	3/9/2010
	<b>First Named Inventor</b>	Rozman et al.
	<b>Title</b>	System and Method for Protecting a Computer System from Malicious Software
	<b>Art Unit</b>	2439
	<b>Examiner Name</b>	Christian A. LaForgia
	<b>Attorney Docket Number</b>	ARC-01RE1

I hereby revoke all previous powers of attorney given in the above-identified application.

A Power of Attorney is submitted herewith.

**OR**

I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: 25962

**OR**

I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified application to:

The address associated with the above-mentioned Customer Number:

**OR**

The address associated with Customer Number:  

**OR**

<input type="checkbox"/> Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone	Email		

I am the:

Applicant/Inventor

Assignee of record of the entire interest. See 37 CFR 3.71.  
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on \_\_\_\_\_

**SIGNATURE of Applicant or Assignee of Record**

Signature		Date	8-11-11
Name	Allen F. Rozman	Telephone	
Title and Company	ARAC		

**NOTE:** Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below\*.

\*Total of \_\_\_\_\_ forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>POWER OF ATTORNEY OR REVOCAION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS</b>	<b>Application Number</b>	12/720,147
	<b>Filing Date</b>	3/9/2010
	<b>First Named Inventor</b>	Rozman et al.
	<b>Title</b>	System and Method for Protecting a Computer System from Malicious Software
	<b>Art Unit</b>	2439
	<b>Examiner Name</b>	Christian A. LaForgia
	<b>Attorney Docket Number</b>	ARC-01RE1

I hereby revoke all previous powers of attorney given in the above-identified application.

A Power of Attorney is submitted herewith.

**OR**

I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: 25962

**OR**

I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified application to:

The address associated with the above-mentioned Customer Number:

**OR**

The address associated with Customer Number:  

**OR**

<input type="checkbox"/> Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone	Email		

I am the:

Applicant/Inventor

Assignee of record of the entire interest. See 37 CFR 3.71.  
Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on \_\_\_\_\_

**SIGNATURE of Applicant or Assignee of Record**

Signature		Date	
Name	Alfonso J. Cioffi	Telephone	
Title and Company	ARAC		

**NOTE:** Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below\*.

\*Total of \_\_\_\_\_ forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	10743498
<b>Application Number:</b>	12720147
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	8473
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Correspondence Address:</b>	Allen F. Rozman - 6402 Wildlife Trail - Garland TX 75044 US 214-478-2172 arozman@verizon.net
<b>Filer:</b>	Glenn W. Boisbrun/Sherry Colgrove
<b>Filer Authorized By:</b>	Glenn W. Boisbrun
<b>Attorney Docket Number:</b>	ARAC-01RE1
<b>Receipt Date:</b>	16-AUG-2011
<b>Filing Date:</b>	09-MAR-2010
<b>Time Stamp:</b>	10:24:02
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	ARC-01RE1_POA.pdf	153227 e8573e2ae3ad0c8a827371d2fd52e010b67c8c1e	no	2

**Warnings:**

**Information:**

<b>Total Files Size (in bytes):</b>	153227
-------------------------------------	--------

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
12/720,147	03/09/2010	Allen F. Rozman	ARC-01RE1

**CONFIRMATION NO. 8473**

**POA ACCEPTANCE LETTER**



25962  
SLATER & MATSIL, L.L.P.  
17950 PRESTON RD, SUITE 1000  
DALLAS, TX 75252-5793

Date Mailed: 08/24/2011

**NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY**

This is in response to the Power of Attorney filed 08/16/2011.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/atesfai/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/720,147	03/09/2010	Allen F. Rozman	ARC-01RE1	8473
25962	7590	08/26/2011	EXAMINER	
SLATER & MATSIL, L.L.P. 17950 PRESTON RD, SUITE 1000 DALLAS, TX 75252-5793			LAFORGIA, CHRISTIAN A	
			ART UNIT	PAPER NUMBER
			2439	
			NOTIFICATION DATE	DELIVERY MODE
			08/26/2011	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docteting@slater-matsil.com

<b>Applicant-Initiated Interview Summary</b>	<b>Application No.</b> 12/720,147	<b>Applicant(s)</b> ROZMAN ET AL.	
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439	

All participants (applicant, applicant's representative, PTO personnel):

- (1) Christian LaForgia. (3) Allen F. Rozman.  
(2) Glenn Boisbrun. (4) \_\_\_\_\_.

Date of Interview: 22 August 2011.

Type:  Telephonic  Video Conference  
 Personal [copy given to:  applicant  applicant's representative]

Exhibit shown or demonstration conducted:  Yes  No.  
If Yes, brief description: \_\_\_\_\_.

Issues Discussed 101 112 102 103 Others  
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1 and 21.

Identification of prior art discussed: US 2002/0002673 (NARIN).

**Substance of Interview**

(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

See Continuation Sheet.

**Applicant recordation instructions:** The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

**Examiner recordation instructions:** Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Attachment

/Christian LaForgia/  
Primary Examiner, Art Unit 2439



## Summary of Record of Interview Requirements

### Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record

A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

### Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews

Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.

All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

- 1) A brief description of the nature of any exhibit shown or any demonstration conducted,
- 2) an identification of the claims discussed,
- 3) an identification of the specific prior art discussed,
- 4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
- 5) a brief identification of the general thrust of the principal arguments presented to the examiner,  
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
- 6) a general indication of any other pertinent matters discussed, and
- 7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

### Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Continuation of Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: The Applicant discussed differences between the cited prior art and the claimed invention. First the Applicant pointed out that prior art does not disclose a first logical process executing on a first processor and a second logical process executing on a second process. The Examiner pointed out that the prior art discloses that the invention may be implemented on a multi-processor system (paragraph 0019) and that the prior art reasonably suggests that the processes operated on separate processors. The Applicant pointed out that the prior art was not specific enough in its disclosure.

The Applicant also argued that the prior art did not teach a first and second browser process (with respect to claim 21). The Applicant pointed out several locations in the prior art where the alleged first process (the secure rendering application) did not actually perform any browser functions and instead invoked a second process (the hosting application) to perform web browsing functions. The Examiner noted that the prior art reference did not define secure rendering application. Furthermore, the prior art's disclosure of secure rendering application is unclear; the prior art states at paragraph 0036 that the "[secure rendering] application 312 may provide some type of web browsing capability to its user, but, rather than performing the actual web browsing itself, application 312 may call upon a general-purpose web browsing program to perform the web-browsing." Based on this disclosure it appears that the secure rendering application may have some browser functionality, since the prior art states that the application may provide some type of web browsing capability and may invoke a general-purpose web browser. There is enough to suggest to one of ordinary skill in the art that the application may provide web browsing capabilities, instead of optionally invoking one. The Applicant kept pointing to locations where the secure rendering application invoked a general-purpose browser. The Examiner and Applicant did not reach an agreement with respect to this limitation. The Examiner will take further action upon receiving a formal response.

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicants: Rozman, *et al.*

Reissue of: 7,484,247

Issued:

January 27, 2009

Title: System and Method for Protecting a Computer System from Malicious Software.

**Agenda for Patent Examiner Interview with Christian LaForgia**  
**August 22, 2011**

- Ser # 12/720,147, Docket # ARAC-01RE1
  - 35 USC § 102 claim rejections
    - Discussion of U.S. Patent Publication 2002/0002673 A1 to Narin
    - Discussion of possible claim amendments
- Ser # 12/941,067, Docket # ARAC-01RE4
  - 35 USC § 251 Improper broadening rejection
  - 35 USC § 102 claim rejections
    - Discussion of U.S. Patent Publication 2002/0002673 A1 to Narin
- Ser # 13/015,186, Docket # ARAC-01RE3C1
  - Specification objection
    - computer readable medium
- Closing and any remaining issue

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicants: Rozman, *et al.*                      Docket No.: ARAC-01RE1  
Serial No.: 12/720,147                              Filed: 03/09/2010  
Reissue of: 7,484,247                                Issued: January 27, 2009  
Title: System and Method for Protecting a Computer System from Malicious Software.

Commissioner for Patents  
P. O. Box 1450  
Alexandria, VA 22313-1450

**AMENDMENT UNDER 37 CFR §1.111**

Dear Sir:

The following amendments and remarks are presented in response to the Examiner's Office Action mailed April 29, 2011. Please amend the above-referenced application as follows. No new matter has been added.

IN THE SPECIFICATION:

Before the heading “Cross Reference to Related Patents and Applications” kindly insert:

Cross Reference to Multiple Reissue Applications

This application is a reissue application of U.S. Patent No. 7,484,247, entitled “System and Method for Protecting a Computer System from Malicious Software,” issued on January 27, 2009, and is related to another reissue application designated U.S. Patent Application Serial No. 12/720,207 from U.S. Patent No. 7,484,247 filed concurrently herewith, which are incorporated herein by reference. This application is also related to another reissue application designated U.S. Patent Application Serial No. 12/854,149 from U.S. Patent No. 7,484,247 filed on August 10, 2010 and a continuation application therefrom designated U.S. Patent Application Serial No. 13/015,186 filed on January 27, 2011, which are incorporated herein by reference. This application is also related to another reissue application designated U.S. Patent Application Serial No. 12/941,067 from U.S. Patent No. 7,484,247 filed on November 7, 2010, which is incorporated herein by reference.

IN THE CLAIMS:

1. (Thrice Amended) A method of operating a computer system capable of exchanging data across a network of one or more computers and having at least a first and second electronic data processor capable of executing instructions using a common operating system, comprising[ the steps of]:

executing a first browser process~~instructions~~ in a first logical process within the common operating system using the first electronic data processor, wherein the first logical process is capable of accessing data contained in a first memory space[ and a second memory space];

executing a second browser process~~instructions~~ in a second logical process within the common operating system using the second electronic data processor, wherein the second logical process is capable of accessing data contained in the second memory space[, the second logical process being further capable of exchanging data across a network of one or more computers];  
and

displaying[, in a windowed format on a display terminal,] data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to [the]a display[ terminal];

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser~~logical~~ process.

2. (Twice Amended) The method of claim 1 wherein the [ first memory space and the] second memory space [comprise separate regions of a common memory space is]comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

3. (Twice Amended) The method of claim 1 wherein the first logical process is capable of accessing data contained in the second memory spaces~~second logical process is selected from the group consisting of:~~

~~———— an electronic mail process, an instant messaging process, an internet browser process, an interactive gaming process, a virtual private network (VPN) process, and a reader application process.~~

4. (Original) The method of claim 1 wherein the first logical process receives user interface data, and passes the user interface data to the second logical process.

5. (Original) The method of claim 1 wherein the first and second electronic data processors are part of a multi-core electronic data processor.

6. (Twice Amended) The method of claim 1 and further comprising[ the step of] restoring at least one corrupted data file[ residing on the second memory space] from [an]a protected image[ residing on the first memory space].

7. (Amended) The method of claim 1 and further comprising[ the step of] automatically deleting at least one data file residing on the second memory space when the second logical process is terminated.

8. (Amended) The method of claim 1 and further comprising[ the steps of]:  
encrypting data with the first logical process;  
transferring the encrypted data from the first logical process to the second logical process; and  
transferring the encrypted data from the second logical process to the network interface device.

9. (Amended) The method of claim 8 and further comprising[ the steps of]:  
decrypting the data with the network interface device; and  
transferring the decrypted data from the network interface device to the network.

10. (Thrice Amended) A multi-processor computer system using a common operating system capable of exchanging data across a network of one or more computers via a network interface device, comprising:

a first electronic data processor capable of executing a first browser process~~instructions~~ using the common operating system and communicatively coupled to a first memory space[ and a second memory space];

a second electronic data processor capable of executing a second browser~~process~~~~instructions~~ using the common operating system and communicatively coupled to [the]a second memory space[ and a network interface device, wherein the second electronic data processor is capable of exchanging data across a network of one or more computers via the network interface device]; and

a video processor adapted to combine video data from the first and second electronic data processors and transmit the combined video data to a display[ terminal for displaying the combines video data in a windowed format];



wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process on the second electronic data processor.

11. (Twice Amended) The computer system of claim 10 wherein the [ first memory space and the] second memory space [ comprise separate regions of a common memory space is] comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

12. (Original) The computer system of claim 10 wherein the first and second electronic data processors are part of a dual processor computer system.

13. (Original) The computer system of claim 10 wherein the second electronic data processor and the video processor are co-located on a circuit card, the circuit card being communicatively coupled to the first electronic data processor.

14. (Original) The computer system of claim 10 wherein the computer system is configured such that the first electronic data processor is protected from executing instructions initiated by a malware process downloaded from the network and executing on the second electronic data processor.

15. (Thrice Amended) A multi-processor computer system using a common operating system capable of exchanging data across a network of one or more computers, comprising:

at least a first and second electronic data processor capable of executing instructions using the common operating system;

at least a first and second memory space; and

a video processor;

wherein the first and second electronic data processors, first and second memory space, and video processor are configured to:[for performing the steps of;]

[executing]execute a first browser processinstructions in a first logical process with the first electronic data processor, wherein the first logical process is executing within the common operating system and is capable of accessing data contained in the first memory space;

[executing]execute a second browser processinstructions in a second logical process with the second electronic data processor, wherein the second logical process is executing within the common operating system and is capable of accessing data contained in the second memory space[, the second logical process being further capable of exchanging data across a network of one or more computers]; and

[displaying, in a windowed format on a display terminal,]display data from the first logical process and the second logical process, wherein the video processor is adapted to combine data from the first and second logical processes and transmit the combined data to [the]a display[ terminal];

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browserlogical process.

16. (Original) The computer system of claim 15 wherein the computer system is further configured such that the first logical process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second logical process.

17. (Twice Amended) The computer system of claim 15 and further comprising[:] at least one network interface device capable of exchanging data with[ both the second logical process and with] the network and with a logical process that comprises a process selected from the group consisting of:

the first logical process; and

the second logical process.

18. (Original) The computer system of claim 17 wherein the network interface device is capable of decrypting data received from the second logical process and transmitting the decrypted data to the network while preventing the second logical process from accessing the decrypted data.

19. (Amended) The computer system of claim 15 wherein the at least one electronic data processor [is]comprises a processor selected from the group consisting of[:] a multi-core electronic data processor; dual electronic data processors; and multiple electronic data processors.

20. (Twice Amended) The computer system of claim 15 and further configured to restore[for performing the step of: restoring] at least one corrupted data file[ residing on the second memory space] from [an]a protected image[ residing on the first memory space].

21. (New) A portable computer capable of executing instructions using a common operating system, comprising:

a network interface device configured to exchange data across a network of one or more computers and access at least one website;

at least a first memory space and a second memory space, the first memory space containing at least one system file;

at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, wherein the user interface is configured to receive input from a computer user;

the at least one electronic data processor configured to execute a first browser process in a first logical process within the common operating system, wherein the first logical process is capable of accessing data contained in the first memory space;

the at least one electronic data processor further configured to execute a second browser process in a second logical process within the common operating system, wherein the second logical process is capable of accessing data contained in the second memory space and is further capable of generating video data from a website accessed via the network; and

a video processor configured to process video data from the second browser process for display;

wherein the first browser process is capable of opening the second browser process and is further capable of passing data to the second browser process;

wherein further the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing within the second browser process.

22. (New) The portable computer of Claim 21 wherein the first browser process is capable of directly exchanging data with the network interface device and with the second browser process.

23. (New) The portable computer of Claim 22 wherein the first browser process is capable of passing data downloaded from the network to the second browser process.

24. (New) The portable computer of Claim 21 wherein the second browser process is capable of directly exchanging data with the network interface device and with the first browser process.

25. (New) The portable computer of Claim 21 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

an Application Specific Integrated Circuit;

a Field Programmable Gate Array;

a plurality of electronic data processors; and

a multi-core electronic data processor.

26. (New) The portable computer of Claim 21 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

27. (New) The portable computer of Claim 21 configured such that at least one corrupted file required for a browser process is capable of being restored from a protected image.

28. (New) The portable computer of Claim 27 wherein the protected image is stored at a location selected from the group consisting of:

a removable drive;

the first memory space;

a partition on a memory device; and

a nonvolatile memory disk.

29. (New) The portable computer of Claim 21 configured such that at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated.

30. (New) The portable computer of Claim 21 configured such that the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.

31. (New) The portable computer of Claim 21 wherein attempts by malware to record data entry by the computer user are effectively blocked.

32. (New) A method of operating a portable computer capable of executing instructions using a common operating system and having at least one electronic data processor communicatively coupled to a first and second memory space and to a network interface device, comprising:

exchanging data across a network of one or more computers with the network interface device and accessing at least one website;

storing at least one system file within the first memory space;

executing a first browser process in a first logical process within the common operating system using the at least one electronic data processor, wherein the first logical process is

configured to access data contained in the first memory space;

executing a second browser process in a second logical process within the common operating system using the at least one electronic data processor, wherein the second logical process is configured to access data contained in the second memory space and is further configured to generate video data;

opening the second browser process on instruction from the first browser process;

passing data from the first browser process to the second browser process; and

displaying website video data from the second browser process;

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process.

33. (New) The method of Claim 32 wherein the portable computer is configured such that the first browser process is capable of directly exchanging data with the network interface device and with the second browser process.

34. (New) The method of Claim 33 and further comprising downloading data from the network and passing the data from the first browser process to the second browser process.

35. (New) The method of Claim 32 wherein the portable computer is configured such that the second browser process is capable of directly exchanging data with the network interface device and with the first browser process.

36. (New) The method of Claim 32 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

37. (New) The method of Claim 32 and further comprising restoring at least one corrupted file from a protected image.

38. (New) The method of Claim 37 wherein the protected image is stored at a location selected from the group consisting of:

a removable drive;

the first memory space;

a partition on a memory device; and

a nonvolatile memory disk.

39. (New) The method of Claim 32 and further comprising deleting at least one corrupted data file residing on the second memory space when the second logical process is terminated.

40. (New) The method of Claim 32 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

an Application Specific Integrated Circuit;

a Field Programmable Gate Array;

a plurality of electronic data processors; and

a multi-core electronic data processor.

41. (New) The method of Claim 32 wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.



42. (New) The method of Claim 32 and further comprising displaying video data from the first browser process.

43. (New) The method of Claim 32 wherein attempts by malware to record data entry by the computer user are effectively blocked.

44. (New) A method of operating a portable computer comprising a network interface device, at least a first memory space and a second memory space, and at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, comprising:

exchanging data across a network of one or more computers with the network interface device and accessing at least one website;

storing at least one system file in the first memory space;

opening a first browser process, wherein the first browser process is capable of accessing data contained in the first memory space;

opening a second browser process, wherein the second browser process is capable of accessing data contained in the second memory space, and is further capable of generating data for video display; and

passing data from the first browser process to the second browser process;

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process.

45. (New) The method of Claim 44 wherein the first browser process is capable of directly exchanging data with the network interface device and with the second browser process.

46. (New) The method of Claim 45 and further comprising downloading data from the network and passing the downloaded data from the first browser process to the second browser process.

47. (New) The method of Claim 46 and further comprising storing the downloaded data on the second memory space.

48. (New) The method of Claim 44 wherein the second browser process is capable of directly exchanging data with the network interface device and with the first browser process.

49. (New) The method of Claim 44 and further comprising restoring at least one corrupted file from a protected image.

50. (New) The method of Claim 49 wherein the protected image is stored at a location selected from the group consisting of:

a removable drive;

the first memory space;

a partition on a memory device; and

a non-volatile memory disk.

51. (New) The method of Claim 44 wherein at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated.

52. (New) The method of Claim 44 wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.

53. (New) The method of Claim 44 and further comprising the first browser process instructing the second browser process to open.

54. (New) The method of Claim 44 wherein attempts by malware to record data entry by a computer user are effectively blocked.

55. (New) The method of Claim 44 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

an Application Specific Integrated Circuit;

a Field Programmable Gate Array;

a plurality of electronic data processors; and

a multi-core electronic data processor.

56. (New) The method of Claim 44 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

57. (New) The method of Claim 44 and further comprising the first browser process opening a plurality of second browser processes.

58. (New) The portable computer of Claim 21 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

59. (New) The portable computer of Claim 58 wherein the network comprises a cellular data carrier network.

60. (New) The method of Claim 32 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

61. (New) The method of Claim 60 wherein the network comprises a cellular data carrier network.

62. (New) The method of Claim 44 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

63. (New) The method of Claim 62 wherein the network comprises a cellular data carrier network.

64. (New) A computer program product comprising a program code stored in a non-transitory computer readable medium operable on computer capable of executing instructions using a common operating system and having at least one electronic data processor communicatively coupled to a first and second memory space and to a network interface device configured to exchange data across a network of one or more computers and access at least one website, configured to:

store at least one system file within the first memory space;

open a first browser process in a first logical process, the first logical process being configured to access data contained in the first memory space;

open a second browser process in a second logical process, the second logical process being configured to access data contained in the second memory space; and

pass data from the first browser process to the second browser process, wherein the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process.

65. (New) The computer program product of Claim 64 wherein the first browser process is capable of opening the second browser process and the program code stored in the

non-transitory computer readable medium is further configured to pass data to the second browser process.

66. (New) The computer program product of Claim 64 wherein the second logical process is configured to generate data for display and the program code stored in the non-transitory computer readable medium is further configured to process website video data from the second browser process.

67. (New) The computer program product of Claim 64 wherein the first browser process is capable of directly exchanging data with the network interface device and the second browser process or the second browser process is capable of directly exchanging data with the network interface device and the first browser process.

68. (New) The computer program product of Claim 64 wherein at least one corrupted file for a browser process is capable of being restored from a protected file.

69. (New) The computer program product of Claim 64 wherein at least one corrupted file residing on the second memory space is capable of being deleted when the second browser process is terminated.

70. (New) The computer program product of Claim 64 wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.

71. (New) The computer program product of Claim 64 wherein attempts by malware to record data entry by a computer user are effectively blocked.

72. (New) The computer program product of Claim 64 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

73. (New) The computer program product of Claim 72 wherein the network comprises a cellular data carrier network.

## REMARKS

The Applicants have carefully considered this application in connection with the Examiner's Office Action and respectfully request reconsideration of this application in view of the foregoing amendments and the following remarks. The Applicants thank the Examiner for the Examiner Interview on August 22, 2011 and have taken into consideration the topics of discussion therein when addressing the objections and rejections to this application.

The Applicants previously submitted Claims 1-73 in the application. While Claims 1, 3, 10 and 15 have been amended, no claims have been cancelled herein. For the Examiner's benefit, the Applicants have provided an Appendix II to clearly show the amendments to the specification and claims from the amendment filed on April 4, 2011. With respect to the specification, the Cross Reference to Multiple Reissue Applications is submitted without markings as no changes have been made from the previous amendment. Also, the Examiner has indicated that Claims 8, 9, 13 and 18 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Accordingly, Claims 1-73 are currently pending in the application.

### **I. Rejections under 35 U.S.C. §102**

The Examiner has rejected Claims 1-5, 7, 10-12, 14-17, 19, 21-26, 29-48, 51-56, 58-67 and 69-73 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent Application Publication No. 2002/0002673 to Narin. As the Examiner is no doubt aware, anticipation requires that each and every limitation of the claimed invention be disclosed in a single prior art reference. The disclosed limitations must either be disclosed expressly or inherently and must be arranged as in the rejected claims.

For the reasons as set forth herein, the Applicants believe that Narin does not disclose a computer system, portable computer, computer program product or related method as recited in ones of independent Claims 1, 10, 15, 21, 32, 44 and 64 of the present application. In particular, the Applicants believe that Narin fails to disclose, among other things, a computer system, portable computer, computer program product or related method configured to execute (or open) first and second browser processes in accordance with at least one electronic data processor, and protect data (or a system file) residing in a first memory space (accessible by the first browser process) from corruption by a malware process executing as part of the second browser process as recited in ones of independent Claims 1, 10, 15, 21, 32, 44 and 64 of the present application.

Narin provides a technique for allowing an open or untrusted application to provide untrusted or open features for a secure application that are not directly implemented within the secure application (or closed application). In accordance therewith, an open or untrusted application is run in a separate, auxiliary process from the closed or protected application. The auxiliary process is created by running a hosting application that has minimal functionality, just enough to be able to host an application and to communicate with the closed process. The auxiliary process is started by the closed process; the closed process controls the lifetime of the auxiliary process and terminates it when the open features that it provides are no longer necessary. (Paragraph [0006].)

In the following excerpt, Narin teaches away from the closed process being a browser process. If the application is trusted, running a browser in-proc may subvert the security scheme of the trusted application. The browser code may not be secure to the same extent as the trusted application. Even if the browser code itself is secure, the browser provides the capability to import executable code from other sources that may not be trusted. If trust is to be maintained,



executable code from unknown sources cannot be given access to the address space of the trusted application and therefore cannot be run in process. (Paragraph [0004].) As it is well settled, a reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference or would be led in a direction divergent from the path that was taken by the applicant. (See, e.g., *Spectralytics v. Cordis Corp.*, Nos. 2009-1564, 2010-1004 (Fed. Cir. 2011) (citing *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994)).)

Narin continues that in a world where computers are increasingly called upon to handle secure or sensitive information, there is a tension between trusted applications and open applications. Trusted applications typically provide a circumscribed set of functions that cannot be extended by a user, which means that such applications can be trusted to handle sensitive content in predictable ways. Open applications, on the other hand, provide a wide range of functionality that is, in some cases, user expandable - some open applications, such as browsers, can execute code that is user-implemented or imported from other sites on the Internet. (Paragraph [0016].)

In the detailed description, Narin discusses how the secure application (the trusted application) makes use of a non-secure software object (the open process or untrusted application), and clearly describes them as being distinct and different from each other. Narin describes a web browser as being an example of such a non-secure software object, meaning that a web browsing program cannot be part of the secure application. Narin clearly says in the first sentence below that the non-secure software object provides a service that is not directly implemented within the secure application. This can only mean that they are separate and distinct from each other.

Secure application 312 uses non-secure software object 322 to perform an action or provide a service that is not directly implemented within application 312. Non-secure software object 322 is non-secure in the sense that its behavior cannot be relied upon; for example, non-secure software object may be a program that imports and runs arbitrary code from a remote, non-authenticatable (possibly nefarious) source. A web browser is an example of such a non-secure software object 322, because it retrieves and executes scripts from remote locations that may or may not be trustworthy. As an example, application 312 may provide some type of web browsing capability to its user, but rather than performing the actual web browsing functions itself, application 312 may call upon a general-purpose browsing program to perform the web browsing. In this exemplary case, non-secure software object 322 is such a web browsing program. (Paragraph [0036].)

Narin continues to draw the clear distinction between a web browser and a secure application, again, clearly teaching away from the secure application ever being a web browser. A web browser is an example of a non-secure object that should not be granted access to an address space where decrypted content or decryption keys may be stored. Although certain commercially-available browsers may be a known quantity that can be trusted not to contain subversive code, one feature of a browser is that it can load and run arbitrary code from unknown sources (*e.g.*, in the form of an ActiveX® control, a JAVA script or applet, *etc.*). Thus, if the browser runs in the same process as a secure rendering application, the browser could be used to unwittingly download an ActiveX® control that would locate a buffer used by the rendering application to store decrypted content and, say, store that content to the hard disk. (Paragraph [0047].)

Narin belabors the point by providing that the secure rendering application may instruct the browsing program to render a list of links that the user may visit. If the user clicks on any of the links, the browsing program will retrieve the web page associated with that link and display it to the user. It should be observed that it is the browsing program, and not the secure rendering application, that performs the retrieval of web pages. It should further be observed that the downloading of an arbitrary web page in the browser does not, in and of itself, compromise the security of the secure rendering application; since the browser executes in the second process, it has no access to the address space of the secure rendering application that runs in the first process. (Paragraph [0049].)

Narin makes the clearest distinction below between the browser and the secure application, referring to the web browsing function as being a separate program running in a separate process. Narin here is clearly teaching away from the secure application and the non-secure application both comprising browser processes. Preferably, integration between the secure rendering application and the browsing program is as transparent as possible. That is, when the user invokes the secure rendering application, the user should not be aware (and likely does not care) that some of the application's function (*i.e.*, the web browsing function, in this case) is being provided by a separate program running in a separate process. (Paragraph [0050].)

Thus, it is quite clear from the excerpts of the reference reproduced above that Narin fails to disclose, among other things, a computer system, portable computer, computer program product or related method configured to execute (or open) first and second browser processes in accordance with at least one electronic data processor, and protect data (or a system file) residing in a first memory space (accessible by the first browser process) from corruption by a malware process executing as part of the second browser process as recited in ones of independent Claims

1, 10, 15, 21, 32, 44 and 64 of the present application. To reiterate, Narin distinguishes a browser program from a secure process, whereas the claimed invention can protect data (or a system file) residing in the first memory space (accessible by first browser process) from corruption by a malware process executing as part of a separate second browser process in accordance with at least one electronic data processor.

While the Applicants believe that the distinctions above overcome the rejection of the claimed subject matter in view of Narin, the Applicants will briefly address the limitations of Narin with respect to the first and second electronic data processors executing the first and second browser processes, respectively, in view of independent Claims 1, 10 and 15 of the present application. As the Examiner correctly points out, Narin does mention that the computing environment may be embodied in configurations including multiprocessor systems. (Paragraph [0019].) This is a simple listing of well known computing systems and does not teach executing the separate processes on separate processors. Moreover, there is no affirmative statement in Narin that the secure application and the web browser (a non-secure software object) thereof are executed (or can be executed) on separate processors and the only embodiment illustrated and described is a single processor running the two applications. In the environment of an embodiment of the present application as embodied in independent Claims 1, 10 and 15, there is a clear advantage to bifurcating the execution of the first and second browser processes on separate electronic data processors. As an example, a higher level of security may be achieved by partitioning the execution of the processes on physically separate processors. Narin is merely silent on the concept and any advantages associated with the same.

Narin, therefore, fails to disclose the limitations of independent Claims 1, 10, 15, 21, 32, 44 and 64, and the claims dependent thereon. Accordingly, the Applicants respectfully request

the Examiner to withdraw the §102 rejection in view thereof with respect to Claims 1-5, 7, 10-12, 14-17, 19, 21-26, 29-48, 51-56, 58-67 and 69-73 of the present application.

## **II. Rejections under 35 U.S.C. §103(a)**

The Examiner has rejected Claims 6, 20, 27, 28, 37, 38, 49, 50 and 68 under 35 U.S.C. § 103(a) as being unpatentable over Narin in view of U.S. Patent No. 7,024,581 to Wang, *et al.* (“Wang”). The Examiner has also rejected Claim 57 under 35 U.S.C. § 103(a) as being unpatentable over Narin. For the reasons as set forth herein, Narin fails to teach or suggest a method of operating a computer system, a multi-processor computer system, a portable computer and method of operating the same, and a computer program product as recited in ones of independent Claims 1, 15, 21, 32, 44 and 64, and Wang fails to cure the deficiencies thereof. Thus, since Narin fails to teach or suggest all of the limitations of independent Claims 1, 15, 21, 32, 44 and 64, and the secondary reference fails to cure the deficiencies thereof, the Examiner cannot establish a *prima facie* case of obviousness of Claims 6, 20, 27, 28, 37, 38, 49, 50, 57 and 68, which depend from ones thereof. Accordingly, the Applicants respectfully request the Examiner to withdraw the §103 rejection with respect to Claims 6, 20, 27, 28, 37, 38, 49, 50, 57 and 68 of the present application.

## **III. Double Patenting**

The Examiner has provisionally rejected Claims 21-73 on the grounds of nonstatutory double patenting over Claims 21-55 of co-pending U.S. Patent Application Serial No. 12/720,207 to Rozman, *et al.* Although the Applicants do not necessarily agree, the Applicant has filed a Terminal Disclaimer herewith directed to U.S. Patent Application Serial No. 12/720,207 in compliance with 37 CFR §1.321 to overcome the Examiner’s rejection thereto.

#### IV. Conclusion

In view of the foregoing amendments and remarks, the Applicants now see all of the claims currently pending in this application to be in condition for allowance and therefore earnestly solicit a Notice of Allowance therefor.

The Applicants request that the Examiner telephone the undersigned attorney of record at (972) 732-1001 if such would further expedite the prosecution of the present application. If the enclosed fees are insufficient, the Commissioner is hereby authorized to charge any additional fees, or credit any overpayments, to Deposit Account No. 50-1065.

Respectfully submitted,

August 29, 2011

Date

/Glenn W. Boisbrun/

Glenn W. Boisbrun  
Attorney for Applicant  
Reg. No. 39,615

Slater & Matsil, L.L.P.  
17950 Preston Rd., Suite 1000  
Dallas, Texas 75252-5793  
Tel. 972-732-1001  
Fax: 972-732-9218

**APPENDIX I**

**STATUS OF CLAIMS AND  
SUPPORT FOR CLAIM CHANGES**

<b>Claims</b>	<b>Status</b>	<b>Support</b>		
1	Thrice Amended	Col 9 lines 30-37 Fig. 1, 190, 195 Col 18 lines 3-5	Col 11 lines 2-4 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67
2	Twice Amended	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
3	Twice Amended	Col 18 lines 6-10		
4	Original			
5	Original			
6	Twice Amended	Fig. 4, 420	Col 12 lines 46-58	
7	Amended	Col 18 lines 49-52		
8	Amended	Col 18 lines 53-60		
9	Amended	Col 18 lines 61-65		
10	Thrice Amended	Col 9 lines 30-37 Fig. 1, 190, 195 Col 18 lines 3-5	Col 11 lines 2-4 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67
11	Twice Amended	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
12	Original			
13	Original			
14	Original			
15	Thrice Amended	Col 9 lines 30-37 Fig. 1, 190, 195	Col 11 lines 2-4 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67
16	Original			
17	Twice Amended	Fig. 1, 120, 191, 190, 110, 130		
18	Original			
19	Amended	Col 20 lines 38-42		
20	Twice Amended	Fig. 4, 420	Col 12 lines 46-58	
21	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53 Fig. 1, 120, 191, 190, 110, 130	Fig. 1, 120, 150, 160 Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Col 11 lines 2-4 Col 8 lines 1-6	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 23-28 Col 18 lines 3-5
22	New	Fig. 1, 120, 191, 190		

23	New	Fig. 1, 120, 191, 190, 195	Col 11 lines 38-41	
24	New	Fig. 1, 140, 190		
25	New	Col 14 lines 62-67	Col 9 lines 30-47	
26	New	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
27	New	Fig. 4, 420	Col 12 lines 46-58	
28	New	Col 12 lines 46-58	Col 7 lines 13-16	
29	New	Col 8 lines 23-26		
30	New	Col 19 lines 33-37		
31	New	Col 7 lines 58-62		
32	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Col 11 lines 2-4 Col 8 lines 1-6	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 23-28
33	New	Fig. 1, 120, 191, 190		
34	New	Fig. 1, 120, 191, 190, 195	Col 11 lines 38-41	
35	New	Fig. 1, 140, 190		
36	New	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
37	New	Fig. 4, 420	Col 12 lines 46-58	
38	New	Col 12 lines 46-58	Col 7 lines 13-16	
39	New	Col 8 lines 23-26		
40	New	Col 14 lines 62-67	Col 9 lines 30-47	
41	New	Col 19 lines 33-37		
42	New	Fig. 1, 120, 170, 171, 180		
43	New	Col 7 lines 58-62		
44	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Col 11 lines 2-4 Col 8 lines 1-6	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 25-28
45	New	Fig. 1, 120, 191, 190		
46	New	Fig. 1, 120, 191, 190, 195	Col 11 lines 38-41	
47	New	Fig. 3, 320		
48	New	Fig. 1, 140, 190		
49	New	Fig. 4, 420	Col 12 lines 46-58	
50	New	Col 12 lines 46-58	Col 7 lines 13-16	
51	New	Col 8 lines 23-26		



52	New	Col 19 lines 33-37		
53	New	Fig 2, 220		
54	New	Col 7 lines 58-62		
55	New	Col 14 lines 62-67	Col 9 lines 30-47	
56	New	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
57	New	Col 13 lines 22-24	Fig 2, 220	
58	New	Col 10 lines 19-22		
59	New	Col 1 and 2	US PAT 6,216,112	
60	New	Col 10 lines 19-22		
61	New	Col 1 and 2	US PAT 6,216,112	
62	New	Col 10 lines 19-22		
63	New	Col 1 and 2	US PAT 6,216,112	
64	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Col 11 lines 2-4 Col 8 lines 1-6	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 25-28
65	New	Fig. 1, 120, 191, 190, 195	Col 11 lines 38-41 Col 13 lines 22-24	Fig 2, 220
66	New	Fig. 1		
67	New	Fig. 1, 120, 191, 190		
68	New	Fig. 4, 420	Col 12 lines 46-58	
69	New	Col 8 lines 23-26		
70	New	Col 19 lines 33-37		
71	New	Col 7 lines 58-62		
72	New	Col 10 lines 19-22		
73	New	Col 1 and 2	US PAT 6,216,112	

## APPENDIX II

### SPECIFICATION AS AMENDED ACCORDING TO STANDARD AMENDMENT FORMAT

No changes have been made to the “Cross Reference to Multiple Reissue Applications” section and, as such, the section is set forth below without markings:

#### Cross Reference to Multiple Reissue Applications

This application is a reissue application of U.S. Patent No. 7,484,247, entitled “System and Method for Protecting a Computer System from Malicious Software,” issued on January 27, 2009, and is related to another reissue application designated U.S. Patent Application Serial No. 12/720,207 from U.S. Patent No. 7,484,247 filed concurrently herewith, which are incorporated herein by reference. This application is also related to another reissue application designated U.S. Patent Application Serial No. 12/854,149 from U.S. Patent No. 7,484,247 filed on August 10, 2010 and a continuation application therefrom designated U.S. Patent Application Serial No. 13/015,186 filed on January 27, 2011, which are incorporated herein by reference. This application is also related to another reissue application designated U.S. Patent Application Serial No. 12/941,067 from U.S. Patent No. 7,484,247 filed on November 7, 2010, which is incorporated herein by reference.

## CLAIMS AS AMENDED ACCORDING TO STANDARD AMENDMENT FORMAT

1. (Currently Amended) A method of operating a computer system capable of exchanging data across a network of one or more computers and having at least a first and second electronic data processor capable of executing instructions using a common operating system, comprising:

executing a first browser process~~instructions~~ in a first logical process within the common operating system using the first electronic data processor, wherein the first logical process is capable of accessing data contained in a first memory space;

executing a second browser process~~instructions~~ in a second logical process within the common operating system using the second electronic data processor, wherein the second logical process is capable of accessing data contained in the second memory space; and

displaying data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to a display;

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser~~logical~~ process.

2. (Previously Presented) The method of claim 1 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;  
random access memory (RAM); and  
both volatile and nonvolatile memory.

3. (Currently Amended) The method of claim 1 wherein the first logical process is capable of accessing data contained in the second memory space~~second logical process~~  
~~comprises a process selected from the group consisting of:~~

~~— an electronic mail process, an instant messaging process, an internet browser process, an interactive gaming process, a virtual private network (VPN) process, and a reader application process.~~

4. (Previously Presented) The method of claim 1 wherein the first logical process receives user interface data, and passes the user interface data to the second logical process.

5. (Previously Presented) The method of claim 1 wherein the first and second electronic data processors are part of a multi-core electronic data processor.

6. (Previously Presented) The method of claim 1 and further comprising restoring at least one corrupted data file from a protected image.

7. (Previously Presented) The method of claim 1 and further comprising automatically deleting at least one data file residing on the second memory space when the second logical process is terminated.

8. (Previously Presented) The method of claim 1 and further comprising:  
encrypting data with the first logical process;  
transferring the encrypted data from the first logical process to the second logical process; and

transferring the encrypted data from the second logical process to the network interface device.

9. (Previously Presented) The method of claim 8 and further comprising:  
decrypting the data with the network interface device; and  
transferring the decrypted data from the network interface device to the network.

10. (Currently Amended) A multi-processor computer system using a common operating system capable of exchanging data across a network of one or more computers via a network interface device, comprising:

a first electronic data processor capable of executing a first browser process~~instructions~~ using the common operating system and communicatively coupled to a first memory space;

a second electronic data processor capable of executing a second browser process~~instructions~~ using the common operating system and communicatively coupled to a second memory space; and

a video processor adapted to combine video data from the first and second electronic data processors and transmit the combined video data to a display;

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process~~on the second electronic data processor~~.

11. (Previously Presented) The computer system of claim 10 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;  
a partition on a memory device;

random access memory (RAM); and  
both volatile and nonvolatile memory.

12. (Previously Presented) The computer system of claim 10 wherein the first and second electronic data processors are part of a dual processor computer system.

13. (Previously Presented) The computer system of claim 10 wherein the second electronic data processor and the video processor are co-located on a circuit card, the circuit card being communicatively coupled to the first electronic data processor.

14. (Previously Presented) The computer system of claim 10 wherein the computer system is configured such that the first electronic data processor is protected from executing instructions initiated by a malware process downloaded from the network and executing on the second electronic data processor.

15. (Currently Amended) A multi-processor computer system using a common operating system capable of exchanging data across a network of one or more computers, comprising:

at least a first and second electronic data processor capable of executing instructions using the common operating system;

at least a first and second memory space; and

a video processor;

wherein the first and second electronic data processors, first and second memory space, and video processor are configured to:

execute a first browser process instructions in a first logical process with the first electronic data processor, wherein the first logical process is executing within the common operating system and is capable of accessing data contained in the first memory space;

execute a second browser process instructions in a second logical process with the second electronic data processor, wherein the second logical process is executing within the common operating system and is capable of accessing data contained in the second memory space; and

display data from the first logical process and the second logical process, wherein the video processor is adapted to combine data from the first and second logical processes and transmit the combined data to a display;

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browerlogical process.

16. (Previously Presented) The computer system of claim 15 wherein the computer system is further configured such that the first logical process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second logical process.

17. (Previously Presented) The computer system of claim 15 and further comprising at least one network interface device capable of exchanging data with the network and with a logical process that comprises a process selected from the group consisting of:

the first logical process; and

the second logical process.

18. (Previously Presented) The computer system of claim 17 wherein the network interface device is capable of decrypting data received from the second logical process and

transmitting the decrypted data to the network while preventing the second logical process from accessing the decrypted data.

19. (Previously Presented) The computer system of claim 15 wherein the at least one electronic data processor comprises a processor selected from the group consisting of a multi-core electronic data processor; dual electronic data processors; and multiple electronic data processors.

20. (Previously Presented) The computer system of claim 15 and further configured to restore-at least one corrupted data file from a protected image.

21. (Previously Presented) A portable computer capable of executing instructions using a common operating system, comprising:

a network interface device configured to exchange data across a network of one or more computers and access at least one website;

at least a first memory space and a second memory space, the first memory space containing at least one system file;

at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, wherein the user interface is configured to receive input from a computer user;

the at least one electronic data processor configured to execute a first browser process in a first logical process within the common operating system, wherein the first logical process is capable of accessing data contained in the first memory space;

the at least one electronic data processor further configured to execute a second browser process in a second logical process within the common operating system, wherein the second logical process is capable of accessing data contained in the second memory space and is further



capable of generating video data from a website accessed via the network; and

a video processor configured to process video data from the second browser process for display;

wherein the first browser process is capable of opening the second browser process and is further capable of passing data to the second browser process;

wherein further the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing within the second browser process.

22. (Previously Presented) The portable computer of Claim 21 wherein the first browser process is capable of directly exchanging data with the network interface device and with the second browser process.

23. (Previously Presented) The portable computer of Claim 22 wherein the first browser process is capable of passing data downloaded from the network to the second browser process.

24. (Previously Presented) The portable computer of Claim 21 wherein the second browser process is capable of directly exchanging data with the network interface device and with the first browser process.

25. (Previously Presented) The portable computer of Claim 21 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

an Application Specific Integrated Circuit;

a Field Programmable Gate Array;

a plurality of electronic data processors; and

a multi-core electronic data processor.

26. (Previously Presented) The portable computer of Claim 21 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

27. (Previously Presented) The portable computer of Claim 21 configured such that at least one corrupted file required for a browser process is capable of being restored from a protected image.

28. (Previously Presented) The portable computer of Claim 27 wherein the protected image is stored at a location selected from the group consisting of:

a removable drive;

the first memory space;

a partition on a memory device; and

a nonvolatile memory disk.

29. (Previously Presented) The portable computer of Claim 21 configured such that at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated.

30. (Previously Presented) The portable computer of Claim 21 configured such that the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.

31. (Previously Presented) The portable computer of Claim 21 wherein attempts by malware to record data entry by the computer user are effectively blocked.

32. (Previously Presented) A method of operating a portable computer capable of executing instructions using a common operating system and having at least one electronic data processor communicatively coupled to a first and second memory space and to a network interface device, comprising:

exchanging data across a network of one or more computers with the network interface device and accessing at least one website;

storing at least one system file within the first memory space;

executing a first browser process in a first logical process within the common operating system using the at least one electronic data processor, wherein the first logical process is configured to access data contained in the first memory space;

executing a second browser process in a second logical process within the common operating system using the at least one electronic data processor, wherein the second logical process is configured to access data contained in the second memory space and is further configured to generate video data;

opening the second browser process on instruction from the first browser process;

passing data from the first browser process to the second browser process; and

displaying website video data from the second browser process;

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process.

33. (Previously Presented) The method of Claim 32 wherein the portable computer is configured such that the first browser process is capable of directly exchanging data with the network interface device and with the second browser process.

34. (Previously Presented) The method of Claim 33 and further comprising downloading data from the network and passing the data from the first browser process to the second browser process.

35. (Previously Presented) The method of Claim 32 wherein the portable computer is configured such that the second browser process is capable of directly exchanging data with the network interface device and with the first browser process.

36. (Previously Presented) The method of Claim 32 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

37. (Previously Presented) The method of Claim 32 and further comprising restoring at least one corrupted file from a protected image.

38. (Previously Presented) The method of Claim 37 wherein the protected image is stored at a location selected from the group consisting of:

a removable drive;

the first memory space;

a partition on a memory device; and

a nonvolatile memory disk.

39. (Previously Presented) The method of Claim 32 and further comprising deleting at least one corrupted data file residing on the second memory space when the second logical process is terminated.

40. (Previously Presented) The method of Claim 32 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

an Application Specific Integrated Circuit;

a Field Programmable Gate Array;

a plurality of electronic data processors; and

a multi-core electronic data processor.

41. (Previously Presented) The method of Claim 32 wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.

42. (Previously Presented) The method of Claim 32 and further comprising displaying video data from the first browser process.

43. (Previously Presented) The method of Claim 32 wherein attempts by malware to record data entry by the computer user are effectively blocked.

44. (Previously Presented) A method of operating a portable computer comprising a network interface device, at least a first memory space and a second memory space, and at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, comprising:

exchanging data across a network of one or more computers with the network interface device and accessing at least one website;

storing at least one system file in the first memory space;

opening a first browser process, wherein the first browser process is capable of accessing data contained in the first memory space;

opening a second browser process, wherein the second browser process is capable of

accessing data contained in the second memory space, and is further capable of generating data for video display; and

passing data from the first browser process to the second browser process;

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process.

45. (Previously Presented) The method of Claim 44 wherein the first browser process is capable of directly exchanging data with the network interface device and with the second browser process.

46. (Previously Presented) The method of Claim 45 and further comprising downloading data from the network and passing the downloaded data from the first browser process to the second browser process.

47. (Previously Presented) The method of Claim 46 and further comprising storing the downloaded data on the second memory space.

48. (Previously Presented) The method of Claim 44 wherein the second browser process is capable of directly exchanging data with the network interface device and with the first browser process.

49. (Previously Presented) The method of Claim 44 and further comprising restoring at least one corrupted file from a protected image.

50. (Previously Presented) The method of Claim 49 wherein the protected image is stored at a location selected from the group consisting of:

a removable drive;

the first memory space;

a partition on a memory device; and  
a non-volatile memory disk.

51. (Previously Presented) The method of Claim 44 wherein at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated.

52. (Previously Presented) The method of Claim 44 wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.

53. (Previously Presented) The method of Claim 44 and further comprising the first browser process instructing the second browser process to open.

54. (Previously Presented) The method of Claim 44 wherein attempts by malware to record data entry by a computer user are effectively blocked.

55. (Previously Presented) The method of Claim 44 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

an Application Specific Integrated Circuit;  
a Field Programmable Gate Array;  
a plurality of electronic data processors; and  
a multi-core electronic data processor.

56. (Previously Presented) The method of Claim 44 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;  
a partition on a memory device;

random access memory (RAM); and  
both volatile and nonvolatile memory.

57. (Previously Presented) The method of Claim 44 and further comprising the first browser process opening a plurality of second browser processes.

58. (Previously Presented) The portable computer of Claim 21 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

59. (Previously Presented) The portable computer of Claim 58 wherein the network comprises a cellular data carrier network.

60. (Previously Presented) The method of Claim 32 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

61. (Previously Presented) The method of Claim 60 wherein the network comprises a cellular data carrier network.

62. (Previously Presented) The method of Claim 44 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

63. (Previously Presented) The method of Claim 62 wherein the network comprises a cellular data carrier network.

64. (Previously Presented) A computer program product comprising a program code stored in a non-transitory computer readable medium operable on computer capable of executing instructions using a common operating system and having at least one electronic data processor communicatively coupled to a first and second memory space and to a network interface device configured to exchange data across a network of one or more computers and access at least one website, configured to:

store at least one system file within the first memory space;



open a first browser process in a first logical process, the first logical process being configured to access data contained in the first memory space;

open a second browser process in a second logical process, the second logical process being configured to access data contained in the second memory space; and

pass data from the first browser process to the second browser process, wherein the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process.

65. (Previously Presented) The computer program product of Claim 64 wherein the first browser process is capable of opening the second browser process and the program code stored in the non-transitory computer readable medium is further configured to pass data to the second browser process.

66. (Previously Presented) The computer program product of Claim 64 wherein the second logical process is configured to generate data for display and the program code stored in the non-transitory computer readable medium is further configured to process website video data from the second browser process.

67. (Previously Presented) The computer program product of Claim 64 wherein the first browser process is capable of directly exchanging data with the network interface device and the second browser process or the second browser process is capable of directly exchanging data with the network interface device and the first browser process.

68. (Previously Presented) The computer program product of Claim 64 wherein at least one corrupted file for a browser process is capable of being restored from a protected file.

69. (Previously Presented) The computer program product of Claim 64 wherein at least one corrupted file residing on the second memory space is capable of being deleted when the second browser process is terminated.

70. (Previously Presented) The computer program product of Claim 64 wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process.

71. (Previously Presented) The computer program product of Claim 64 wherein attempts by malware to record data entry by a computer user are effectively blocked.

72. (Previously Presented) The computer program product of Claim 64 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

73. (Previously Presented) The computer program product of Claim 72 wherein the network comprises a cellular data carrier network.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING  
REJECTION OVER A "PRIOR" PATENT**

ARAC-01RE1

In re Application of: Rozman, et al.

Application No.: 12/720,147

Filed: March 9, 2010

For: System and Method for Protecting a Computer System from Malicious Software

The owner\*, Rozman & Cioffi, of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term prior patent Application No. 12/720,207 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1.  For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2.  The undersigned is an attorney or agent of record. Reg. No. 39,615

/Glenn W. Boisbrun/

Signature

August 29, 2011

Date

Glenn W. Boisbrun

Typed or printed name

972-732-1001

Telephone Number

- Terminal disclaimer fee under 37 CFR 1.20(d) included.

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

\*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).

Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	12720147
<b>Filing Date:</b>	09-Mar-2010
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Filer:</b>	Glenn W. Boisbrun/Sherry Colgrove
<b>Attorney Docket Number:</b>	ARAC-01RE1

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				
Extension - 1 month with \$0 paid	2251	1	65	65

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
Statutory or terminal disclaimer	2814	1	70	70
<b>Total in USD (\$)</b>				<b>135</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	10838561
<b>Application Number:</b>	12720147
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	8473
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Customer Number:</b>	25962
<b>Filer:</b>	Glenn W. Boisbrun/Sherry Colgrove
<b>Filer Authorized By:</b>	Glenn W. Boisbrun
<b>Attorney Docket Number:</b>	ARAC-01RE1
<b>Receipt Date:</b>	29-AUG-2011
<b>Filing Date:</b>	09-MAR-2010
<b>Time Stamp:</b>	19:36:10
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$135
RAM confirmation Number	5536
Deposit Account	501065
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	ARAC-01RE1_EOT.pdf	30203 e8e01ec1ffc60a2e687b5733dd881e8f8b942889	no	1

**Warnings:**

**Information:**

2		ARAC-01RE1_Amendment.pdf	168113 4975fe737bd2cf02671d0de43af5c6ca18b6bb9f	yes	47
---	--	--------------------------	--	-----	----

**Multipart Description/PDF files in .zip description**

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Specification	2	2
Claims	3	19
Applicant Arguments/Remarks Made in an Amendment	20	47

**Warnings:**

**Information:**

3	Terminal Disclaimer Filed	ARAC-01RE1_Terminal_Disclaimer.pdf	22305 ce9ae7650361a4348e849ea5951311c1f7d861ba	no	1
---	---------------------------	------------------------------------	---	----	---

**Warnings:**

**Information:**

4	Fee Worksheet (SB06)	fee-info.pdf	32338 3ff69a745af5ef1f83b15b31e8ee2d9fb284632c	no	2
---	----------------------	--------------	---	----	---

**Warnings:**

**Information:**

<b>Total Files Size (in bytes):</b>			252959		
-------------------------------------	--	--	--------	--	--

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**



Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)</b> <b>FY 2009</b> <i>(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)</i>		Docket Number (Optional) ARAC-01RE1	
Application Number <b>12/720,147</b>		Filed <b>3/9/2010</b>	
For <b>System and Method for Protecting a Computer System from Malicious Software</b>			
Art Unit <b>2439</b>		Examiner <b>Christian A. LaForgia</b>	
This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.			
The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):			
	<u>Fee</u>	<u>Small Entity Fee</u>	
<input checked="" type="checkbox"/> One month (37 CFR 1.17(a)(1))	\$ 130	\$ 65	\$ <u>65.00</u>
<input type="checkbox"/> Two months (37 CFR 1.17(a)(2))	\$ 490	\$ 245	\$ _____
<input type="checkbox"/> Three months (37 CFR 1.17(a)(3))	\$ 1,110	\$ 555	\$ _____
<input type="checkbox"/> Four months (37 CFR 1.17(a)(4))	\$ 1,730	\$ 865	\$ _____
<input type="checkbox"/> Five months (37 CFR 1.17(a)(5))	\$ 2,350	\$ 1,175	\$ _____
<input checked="" type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27.			
<input type="checkbox"/> A check in the amount of the fee is enclosed.			
<input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.			
<input checked="" type="checkbox"/> The Director has already been authorized to charge fees in this application to a Deposit Account.			
<input checked="" type="checkbox"/> The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number <u>50-1065</u> .			
<b>WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.</b>			
I am the <input type="checkbox"/> applicant/inventor.			
<input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).			
<input checked="" type="checkbox"/> attorney or agent of record. Registration Number <u>39615</u>			
<input type="checkbox"/> attorney or agent under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 <u>  </u> .			
<u>/Glenn W. Boisbrun/</u>		<u>August 29, 2011</u>	
Signature		Date	
<u>Glenn W. Boisbrun</u>		<u>972-732-1001</u>	
Typed or printed name		Telephone Number	
NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.			
<input type="checkbox"/> Total of _____ forms are submitted.			

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number <b>12/720,147</b>	Filing Date <b>03/09/2010</b>	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (j), or (m))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A		N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(j))</small>	minus 20 =	*	X \$ =	OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =		X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>						
			TOTAL		TOTAL	

\* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR		
AMENDMENT	08/29/2011	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 73	Minus	** 73	=		OR	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	* 7	Minus	***7	=		OR	X \$ =
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE

	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	*	Minus	**	=		OR	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus	***	=		OR	X \$ =
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:  
 /ELMIRA HALL/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449A/PTO				<b>Complete if Known</b>	
<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>				Application Number	12/720,147
<i>(Use as many sheets as necessary)</i>				Filing Date	March 9, 2010
				First Named Inventor	Rozman, et al.
				Art Unit	2439
				Examiner Name	Christian A. LaForgia
Sheet	1	of	1	Attorney Docket Number	ARAC-01RE1

U.S. PATENT DOCUMENTS					
Examiner Initials*	Cite No. <sup>1</sup>	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number - Kind Code <sup>2</sup> (if known)			
	1	US-6,183,366 B1	02-06-2001	Goldberg et al.	
	2	US-6,285,987 B1	09-04-2001	Roth et al.	
	3	US-2004/0199763 A1	10-07-2004	Freund	
	4	US-6,990,630 B2	01-24-2006	Landsman et al.	
	5	US-7,676,842 B2	03-09-2010	Carmona et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No. <sup>1</sup>	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	† <sup>6</sup>
		Country Code <sup>3</sup> - Number <sup>4</sup> - Kind Code <sup>5</sup> (if known)				

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup>Applicant's unique citation designation number (optional). <sup>2</sup>See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup>Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup>For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup>Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup>Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	12720147
<b>Filing Date:</b>	09-Mar-2010
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Filer:</b>	Glenn W. Boisbrun/Sherry Colgrove
<b>Attorney Docket Number:</b>	ARAC-01RE1

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
Submission- Information Disclosure Stmt	1806	1	180	180
<b>Total in USD (\$)</b>				<b>180</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	10871289
<b>Application Number:</b>	12720147
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	8473
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Customer Number:</b>	25962
<b>Filer:</b>	Glenn W. Boisbrun
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	ARAC-01RE1
<b>Receipt Date:</b>	02-SEP-2011
<b>Filing Date:</b>	09-MAR-2010
<b>Time Stamp:</b>	14:44:55
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$180
RAM confirmation Number	1072
Deposit Account	501065
Authorized User	


The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

<b>File Listing:</b>					
<b>Document Number</b>	<b>Document Description</b>	<b>File Name</b>	<b>File Size(Bytes)/ Message Digest</b>	<b>Multi Part /.zip</b>	<b>Pages (if appl.)</b>
1	Transmittal Letter	ARAC-01RE1_IDS_Transmittal.pdf	15964 b6d790987fb006209f07f11b14243c4ef3d49be7	no	1
<b>Warnings:</b>					
<b>Information:</b>					
2	Information Disclosure Statement (IDS) Form (SB08)	ARAC-01RE1_IDS.pdf	71560 11f074495783cbb6d5cbbd4c7232db1321a49306	no	1
<b>Warnings:</b>					
<b>Information:</b>					
This is not an USPTO supplied IDS fillable form					
3	Fee Worksheet (SB06)	fee-info.pdf	30503 98fd3ef485b6f9864b337c9281258003afd2f0	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			118027		
<p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  <b>If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</b></p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  <b>If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</b></p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  <b>If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</b></p>					





<b>Application Number</b> 	<b>Application/Control No.</b> 12/720,147	<b>Applicant(s)/Patent under Reexamination</b> ROZMAN ET AL.	

<b>Document Code - DISQ</b>	<b>Internal Document – DO NOT MAIL</b>
-----------------------------	--

<b>TERMINAL DISCLAIMER</b>	<input type="checkbox"/> APPROVED	<input checked="" type="checkbox"/> DISAPPROVED
Date Filed : 8/29/11	<b>This patent is subject to a Terminal Disclaimer</b>	

**Approved/Disapproved by:**

Felicia D. Roberts  
 Wrong form used: Please use PTO/SB/25



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
12/720,147 03/09/2010 Allen F. Rozman ARAC-01RE1 8473

25962 7590 11/14/2011
SLATER & MATSIL, L.L.P.
17950 PRESTON RD, SUITE 1000
DALLAS, TX 75252-5793

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT PAPER NUMBER

2439

NOTIFICATION DATE DELIVERY MODE

11/14/2011

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@slater-matsil.com



Art Unit: 2439

### **DETAILED ACTION**

1. The amendment of 29 August 2011 has been noted and made of record.
2. Claims 1-73 have been presented for examination.

#### ***Response to Arguments***

3. Applicant's arguments with respect to the prior art rejections, filed 29 August 2011, have been fully considered but they are not persuasive.
4. The Applicant argues that the prior art reference, Narin, does not disclose the claimed invention. Specifically, the Applicant argues that Narin's disclosure of the secure application teaches away from the first browser process. The Examiner disagrees.
5. Throughout his arguments, the Applicant makes reference that the first browser process is a web process. It is noted that the features upon which applicant relies, that the claimed browsers are actually web browsers, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).
6. Despite the Applicant's arguments that the claimed browser is a web browser, the specification appears to give the term a broader meaning. Column 14, lines 27-45 and column 16, lines 25-30 of the Applicant's specification describe the first logical process as being a video game and "including but not [being] limited to a word processor," respectively. According to the Applicant's specification, the claimed first logical process or first browser process could include a web browser, such as Internet Explorer or Netscape; a video game; or a word processor.
7. At the very least, the prior art's disclosure reads on the Applicant's video game and word processor interpretations of browser. Video games are met by the prior art's disclosure of a

Art Unit: 2439

secure rendering application since video games are applications that render interactive environments for users. Furthermore, the Applicant's preferred embodiment in column 16, lines 25-30 appears to be clearly anticipated by the Narin reference. The secure rendering application of Narin meets the limitation of the first browser process in a first logical process when it is interpreted in accordance with this preferred embodiment. Therefore, the secure rendering application of the prior art does teach the first browser process in a first logical process when that limitation is interpreted in light of the specification to include web browsers, video games, and word processing applications.

8. Furthermore, the prior art's disclosure of the secure rendering application is functionally equivalent to the Applicant's claimed first browser process in a first logical process. It is noted that the features upon which applicant relies, such as the first browser process accessing Internet sites and/or data, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). The claims only require that the first browser process in a logical first process "is capable of accessing data contained in a first memory space" and being displayed in combination with the second logical process. As shown below, Narin discloses "a first browser process in a first logical process within the common operating system . . . wherein the first logical process is capable of accessing data contained in a first memory space" in at least figure 2 and paragraphs 0030 and 0031. Narin also shows the first and second logical processes being combined in a display in at least figure 5, the abstract of the patent, and paragraph 0007. Therefore, the secure rendering application of Narin is at least functionally equivalent to the first browser process in a first logical process.

Art Unit: 2439

9. The Applicant also argues that prior art does not teach the first and second browser processes being executed on first and second electronic data processors, respectively. The Examiner disagrees and argues that a prior art reference “may be relied upon for all that it would have reasonably suggested to one having ordinary skill in the art . . . .” M.P.E.P. § 2123; *Merck & Co. v. Biocraft Laboratories*, 874 F.2d 804 (Fed. Cir.), *cert. denied*, 493 U.S. 975 (1989). Narin discloses in paragraph 0019 that the prior art invention may be implemented in multiprocessor systems. Figure 2 illustrates the processes being executed separately, akin to being on separate processes. Based on at least these two sections, the prior art’s disclosure reasonably suggests a technique for implementing the claimed invention in a multi-processor system, where the processes are executed on their own respective processor.

10. See further prior art rejections set forth below.

***Information Disclosure Statement***

11. The information disclosure statement (IDS) submitted on 02 September 2011 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

***Terminal Disclaimer***

12. The terminal disclaimer filed on 29 August 2011 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of 12/720,207 has been reviewed and is NOT accepted.

13. The Applicant used form PTO/SB/26, which is incorrect since the double patenting rejection is not over a prior patent, but instead a co-pending application. The proper form is PTO/SB/25. Appropriate correction is required.

Art Unit: 2439

***Claim Rejections - 35 USC § 102***

14. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

15. Claims 1, 2, 4, 5, 7, 10-12, 14-17, 19, 21-26, 29-48, 51-56, 58-67, and 69-73 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent Application Publication No. 2002/0002673 A1 to Narin, hereinafter Narin.

16. As per claim 1, Narin teaches a method of operating a computer system capable of exchanging data across a network of one or more computers and having at least a first and second electronic data processor capable of executing instructions using a common operating system, comprising the steps of:

executing a first browser process in a first logical process within the common operating system using the first electronic data processor, wherein the first logical process is capable of accessing data contained in a first memory space (Figures 2 [element 210, 212], 3 [element 310]), 4 [step 402], paragraphs 0019, 0030, 0031, 0035, 0036, 0040, 0046, i.e. secure application);

executing a second browser process in a second logical process within the common operating system using the second electronic data processor, wherein the second logical process is capable of accessing data contained in the second memory space (Figures 2 [elements 220, 222], 3 [element 320], 4 [step 404], paragraphs 0019, 0032, 0037, 0040-0041, 0050-0051); and

displaying data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to a display (Figures 1 [element 190], 5, Abstract, paragraphs 0007,

Art Unit: 2439

0050, 0051, the second process renders its output in a child window of the first process, so that the use of a second process to host non-secure software objects is transparent to the user of the first process);

wherein the computer system is configured such that data residing on the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process (Abstract, paragraph 0035-0036, 0039, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

17. Regarding claim 2, Narin teaches wherein the second memory space comprises memory selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figure 2 [element 141], paragraph 0025); a partition on a memory device; random access memory (RAM) (Figure 2 [element 132], paragraph 0023); both volatile and nonvolatile memory.

18. Regarding claim 4, Narin teaches wherein the first logical process receives user interface data and passes the user interface data to the second logical process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042).



Art Unit: 2439

19. Regarding claim 5, Narin teaches wherein the first and second electronic data processors are part of a multi-core electronic data processor (paragraph 0019, multi-core electronic data processor is the functional equivalent of a multiprocessor system, neatly packaged in a single-chip).

20. Regarding claim 7, Narin teaches automatically deleting at least one data file residing on the second memory space when the second logical process is terminated (Figure 4 [step 412], paragraph 0044).

21. As per claims 10 and 15, Narin teaches a multiprocessor computer system (Figure 1 [element 120], paragraphs 0019, 0021, multiprocessor systems) using a common operating system capable of exchanging data across a network of one or more computers via a network interface device, comprising:

a first electronic data processor capable of executing a first browser process using the common operating system and communicatively coupled to a first memory space (Figures 2 [element 210, 212], 3 [element 310]], 4 [step 402], paragraphs 0019, 0030, 0031, 0035, 0036, 0040, 0046, i.e. secure application);

a second electronic data processor capable of executing a second browser process using the common operating system and communicatively coupled to a second memory space (Figures 2 [elements 220, 222], 3 [element 320], 4 [step 404], paragraphs 0019, 0032, 0037, 0040-0041, 0050-0051);

Art Unit: 2439

a video processor adapted to combine video data from the first and second electronic processors and transmit the combined video data to a display (Figures 1 [element 190], 5, Abstract, paragraphs 0007, 0050, 0051, the second process renders its output in a child window of the first process, so that the use of a second process to host non-secure software objects is transparent to the user of the first process);

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first electronic memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process (Abstract, paragraph 0035-0036, 0039, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

22. Regarding claim 11, Narin teaches wherein the second memory space comprises memory selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figure 2 [element 141], paragraph 0025); a partition on a memory device; random access memory (RAM) (Figure 2 [element 132], paragraph 0023); both volatile and nonvolatile memory.

23. Regarding claim 12, Narin teaches wherein the first and second electronic data processors are part of a dual processor computer system (Figure 1 [element 120], paragraphs 0019, 0021, multiprocessor systems).

Art Unit: 2439

24. Regarding claims 14 and 16, Narin teaches wherein the computer system is configured such that the first electronic data processor is protected from executing instructions initiated by a malware process downloaded from the network and executing on the second electronic data processor (Abstract, paragraph 0035-0036, 0039, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

25. Regarding claim 17, Narin teaches at least one network interface device capable of exchanging data with the network and with a logical process selected from the group consisting of: the first logical process and the second logical process (paragraph 0036, secure application 312 may provide some type of web-browsing functionality, which would require exchanging data with the network interface device).

26. Regarding claim 19, Narin teaches wherein the at least one electronic data processor comprises a processor selected from the group consisting of: a multi-core electronic data processor; dual electronic data processors (Figure 1 [element 120], paragraphs 0019, 0021, multiprocessor systems).

27. As per claim 21, Narin teaches a portable computer capable of executing instructions using a common operating system (paragraph 0019, i.e. handheld or laptop devices), comprising:

Art Unit: 2439

a network interface device (Figure 1 [element 170]) configured to exchange data across a network of one or more computers and access at least one website (paragraphs 0026, 0027, 0048, 0049);

at least a first memory space (Figure 2 [elements 132, 141, 212]) and a second memory space (Figure 2 [elements 132, 141, 222]), the first memory space containing at least one system file (Figure 1 [element 134], paragraphs 0030, 0031);

at least one electronic data processor (Figure 1 [element 120]) communicatively coupled (Figure 1 [element 121], system bus) to the network interface device (Figure 1 [element 170]), the first (Figure 2 [elements 132, 141, 212]) and second memory space (Figure 2 [elements 132, 141, 222]), and to a user interface, wherein the user interface is configured to receive input from a computer user (Figure 1 [element 160], paragraph 0025);

the at least one electronic data processor configured to execute a first browser process in a first logical process, wherein the first logical process is capable of accessing data contained in the first memory space (Figures 2 [element 210, 212], 3 [element 310]), 4 [step 402], paragraphs 0030, 0031, 0035, 0036, 0040, 0046, i.e. secure application);

the at least one electronic data processor further configured to execute a second browser process in a second logical process within the common operating system (Figures 2 [element 220], 3 [element 320], 4 [step 404], paragraphs 0032, 0037, 0040), wherein the second logical process is capable of accessing data contained in the second memory space (Figure 2 [elements 220, 222]) and is further capable of generating video data from a website access via the network (Figures 3 [element 322], 4 [steps 406, 410], paragraphs 0040-0041, 0050-0051, rendering

Art Unit: 2439

webpage data, which one of ordinary skill in the art would construe as containing video data, in the non-secure process);

a video processor (Figure 1 [element 190]) configured to transmit video data from the second browser process to a display (Figure 5, Abstract, paragraphs 0007, 0050, 0051, the second process renders its output in a child window of the first process, so that the use of a second process to host non-secure software objects is transparent to the user of the first process);

wherein the first browser process is capable of opening the second browser process and is further capable of passing data to the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application may initiate the hosting of the non-secure software object by instructing the host application to load and execute a non-secure software object within the separate process);

wherein further the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing within the second browser process (Abstract, paragraph 0035-0036, 0039, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

28. Regarding claim 22, Narin teaches wherein the first browser process is capable of exchanging data with the network interface device (paragraph 0036, secure application 312 may provide some type of web-browsing functionality, which would require exchanging data with the network interface device) and with the second browser process (Figures 3 [elements 326, 238], 4

Art Unit: 2439

[step 408], paragraphs 0037-0038, 0041-0042, secure application communicates with hosting application, which hosts non-secure objects).

29. With regards to claim 23, Narin teaches wherein the first browser process is capable of passing data downloaded from the network to the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042).

30. Regarding claim 24, Narin teaches wherein the second browser process is capable of exchanging data with the network interface device (paragraph 0036, non-secure software object is a web browser, which includes the second process exchanging data via the network interface device) and with the first browser process (Figure 5, Abstract, paragraphs 0007, 0050, 0051, the second process communicates with the first process for the purpose of rendering its output in a child window of the first process).

31. Regarding claim 25, Narin teaches wherein the at least one electronic data processor is selected from the group consisting of: an Application Specific Integrated Circuit; a Field Programmable Gate Array; a plurality of electronic data processors (Figure 1 [element 120], paragraphs 0019, 0021, multiprocessor systems); a multi-core electronic data processor.

32. Regarding claim 26, Narin teaches wherein the second memory space is selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figure 2 [element 141], paragraph 0025); a partition on a memory device; random access

Art Unit: 2439

memory (RAM) (Figure 2 [element 132], paragraph 0023); both volatile and nonvolatile memory.

33. Regarding claim 29, Narin teaches at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated (Figure 4 [step 412], paragraph 0044).

34. Regarding claim 30, Narin teaches that the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process (Abstract, paragraph 0035-0036, the first process's address space is inaccessible to the second process).

35. Regarding claim 31, Narin teaches wherein attempts by malware to record data entry by the computer user are effectively blocked (paragraph 0035, provide defense against observation and/or modification).

36. As per claim 32, Narin teaches a method of operating a portable computer (paragraph 0019, i.e. handheld or laptop devices) capable of executing instructions using a common operating system and having at least one electronic data processor (Figure 1 [element 120]) communicatively coupled (Figure 1 [element 121], system bus) to a first (Figure 2 [elements 132, 141, 212]) and second memory space (Figure 2 [elements 220, 222]) and to a network interface device (Figure 1 [element 170]), comprising:

Art Unit: 2439

exchanging data across a network of one or more computers with the network interface device and accessing at least one website (paragraphs 0026, 0027, 0048, 0049);

storing at least one system file within the first memory space (Figures 1 [element 134], 2 [elements 132, 141, 212], paragraphs 0030, 0031);

executing a first browser process in a first logical process within the common operating system using the at least one electronic data processor, wherein the first logical process is configured to access data contained in the first memory space (Figures 2 [element 210, 212], 3 [element 310]), 4 [step 402], paragraphs 0030, 0031, 0035, 0036, 0040, 0046, i.e. secure application);

executing a second browser process in a second logical process within the common operating system using the at least one electronic data processor (Figures 2 [element 220], 3 [element 320], 4 [step 404], paragraphs 0032, 0037, 0040), wherein the second logical process is configured to access data contained in the second memory space (Figure 2 [elements 220, 222]) and is further configured to generate video data (Figures 3 [element 322], 4 [steps 406, 410], paragraphs 0040-0041, 0050-0051, rendering webpage data, which one of ordinary skill in the art would construe as containing video data, in the non-secure process);

opening the second browser process on instruction from the first browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application may initiate the hosting of the non-secure software object by instructing the host application to load and execute a non-secure software object within the separate process);



Art Unit: 2439

passing data from the first browser process to the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application communicates with hosting application, which hosts non-secure objects);

displaying website video data from the second browser process (Figure 5, Abstract, paragraphs 0007, 0050, 0051, the second process renders its output in a child window of the first process, so that the use of a second process to host non-secure software objects is transparent to the user of the first process);

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process (Abstract, paragraph 0035-0036, 0039, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

37. Regarding claim 33, Narin teaches wherein the portable computer is configured such that the first browser process is capable of exchanging data with the network interface device (paragraph 0036, secure application 312 may provide some type of web-browsing functionality, which would require exchanging data with the network interface device) and with the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application communicates with hosting application, which hosts non-secure objects).

38. With regards to claim 34, Narin teaches downloading data from the network and passing

Art Unit: 2439

the data from the first browser process to the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042).

39. Regarding claim 35, Narin teaches wherein the portable computer is configured such that the second browser process is capable of directly exchanging data with the network interface device (paragraph 0036, non-secure software object is a web browser, which includes the second process exchanging data via the network interface device) and with the first browser process (Figure 5, Abstract, paragraphs 0007, 0050, 0051, the second process communicates with the first process for the purpose of rendering its output in a child window of the first process).

40. Regarding claim 36, Narin teaches wherein the second memory space is selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figure 2 [element 141], paragraph 0025); random access memory (RAM) (Figure 2 [element 132], paragraph 0023); both volatile and nonvolatile memory.

41. Regarding claim 39, Narin teaches deleting at least one corrupted data file residing on the second memory space when the second logical process is terminated (Figure 4 [step 412], paragraph 0044).

42. Regarding claim 40, Narin teaches wherein the at least one electronic data processor is selected from the group consisting of: an Application Specific Integrated Circuit; a Field Programmable Gate Array; a plurality of electronic data processors (Figure 1 [element 120],

Art Unit: 2439

paragraphs 0019, 0021, multiprocessor systems); a multi-core electronic data processor.

43. Regarding claim 41, Narin teaches wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process (Abstract, paragraph 0035-0036, the first process's address space is inaccessible to the second process).

44. Regarding claim 42, Narin teaches displaying video data from the first browser process (Figure 5, Abstract, paragraphs 0007, 0050, 0051, the second process renders its output in a child window of the first process, so that the use of a second process to host non-secure software objects is transparent to the user of the first process).

45. Regarding claim 43, Narin teaches wherein attempts by malware to record data entry by the computer user are effectively blocked (paragraph 0035, provide defense against observation and/or modification).

46. As per claims 44 and 64, Narin teaches a method of and non-transitory computer readable medium containing instructions for operating a portable computer (paragraph 0019, i.e. handheld or laptop devices) comprising a network interface device (Figure 1 [element 170]), at least a first memory space (Figure 2 [elements 132, 141, 212]) and a second memory space (Figure 2 [elements 220, 222]), and at least one electronic data processor communicatively coupled (Figure

Art Unit: 2439

1 [element 121], system bus) to the network interface device, the first and second memory space, and to a user interface, comprising:

exchanging data across a network of one or more computers with the network interface device and accessing at least one website (paragraphs 0026, 0027, 0048, 0049);

storing at least one system file in the first memory space (Figures 1 [element 134], 2 [elements 132, 141, 212], paragraphs 0030, 0031);

opening a first browser process, wherein the first browser process is capable of accessing data contained in the first memory space (Figures 2 [element 210, 212], 3 [element 310]), 4 [step 402], paragraphs 0030, 0031, 0035, 0036, 0040, 0046, i.e. secure application);

opening a second browser process (Figures 2 [element 220], 3 [element 320], 4 [step 404], paragraphs 0032, 0037, 0040), wherein the second browser process is capable of accessing data contained in the second memory space (Figure 2 [elements 220, 222]), and is further capable of generating data for video display (Figures 3 [element 322], 4 [steps 406, 410], paragraphs 0040-0041, 0050-0051, rendering webpage data, which one of ordinary skill in the art would construe as containing video data, in the non-secure process);

passing data from the first browser process to the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application communicates with hosting application, which hosts non-secure objects);

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second browser process (Abstract, paragraph 0035-0036, the first process's address space is inaccessible to the second process; provides defense

Art Unit: 2439

against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

47. Regarding claim 45, Narin teaches wherein the first browser process is capable of exchanging data with the network interface device (paragraph 0036, secure application 312 may provide some type of web-browsing functionality, which would require exchanging data with the network interface device) and with the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application communicates with hosting application, which hosts non-secure objects).

48. With regards to claim 46, Narin teaches downloading data from the network and passing the downloaded data from the first browser process to the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042).

49. Concerning claim 47, Narin teaches storing the downloaded data on the second memory space (paragraph 0036, non-secure software object runs web-browsing which includes downloading data).

50. Regarding claim 48, Narin teaches wherein the second browser process is capable of exchanging data with the network interface device (paragraph 0036, non-secure software object is a web browser, which includes the second process exchanging data via the network interface device) and with the first browser process (Figure 5, Abstract, paragraphs 0007, 0050, 0051, the

Art Unit: 2439

second process communicates with the first process for the purpose of rendering its output in a child window of the first process).

51. Regarding claim 51, Narin teaches that at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated (Figure 4 [step 412], paragraph 0044).

52. Regarding claim 52, Narin teaches wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process (Abstract, paragraph 0035-0036, 0039, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

53. Regarding claim 53, Narin teaches the first browser process instructing the second browser process to open (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application may initiate the hosting of the non-secure software object by instructing the host application to load and execute a non-secure software object within the separate process).

54. Regarding claim 54, Narin teaches wherein attempts by malware to record data entry by the computer user are effectively blocked (paragraph 0035, provide defense against observation

Art Unit: 2439

and/or modification).

55. Regarding claim 55, Narin teaches wherein the at least one electronic data processor comprises a processor selected from the group consisting of: an Application Specific Integrated Circuit; a Field Programmable Gate Array; a plurality of electronic data processors (Figure 1 [element 120], paragraphs 0019, 0021, multiprocessor systems); a multi-core electronic data processor.

56. Regarding claim 56, Narin teaches wherein the second memory space comprises memory selected from the group consisting of: a memory zone within a physical memory common to the first memory space (Figure 2 [element 141], paragraph 0025); a partition on a memory device; random access memory (RAM) (Figure 2 [element 132], paragraph 0023); both volatile and nonvolatile memory.

57. Regarding claims 58, 60, 62, and 72, Narin teaches wherein the network interface is capable of exchanging data with the network using a wireless connection (paragraph 0022, wireless media).

58. With regards to claims 59, 61, 63, and 73, Narin teaches wherein the network comprises a cellular data carrier network (paragraph 0022, cellular networks use RF, or radio frequency).

Art Unit: 2439

59. Regarding claim 65, Narin teaches wherein the first browser process is capable of opening the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application may initiate the hosting of the non-secure software object by instructing the host application to load and execute a non-secure software object within the separate process) and the program code stored in the non-transitory computer readable medium is further configured to pass data to the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042).

60. Regarding claim 66, Narin teaches wherein the second logical process is configured to generate data for display and the program code stored in the non-transitory computer readable medium is further configured to process website video data from the second browser process (Figures 3 [element 322], 4 [steps 406, 410], paragraphs 0040-0041, 0050-0051, rendering webpage data, which one of ordinary skill in the art would construe as containing video data, in the non-secure process).

61. Regarding claim 67, Narin teaches wherein the first browser process is capable of directly exchanging data with the network interface device (paragraph 0036, secure application 312 may provide some type of web-browsing functionality, which would require exchanging data with the network interface device) and the second browser process (Figures 3 [elements 326, 238], 4 [step 408], paragraphs 0037-0038, 0041-0042, secure application communicates with hosting application, which hosts non-secure objects) or the second browser process is capable of directly exchanging data with the network interface device (paragraph 0036, non-secure software object



Art Unit: 2439

is a web browser, which includes the second process exchanging data via the network interface device) and the first browser process (Figure 5, Abstract, paragraphs 0007, 0050, 0051, the second process communicates with the first process for the purpose of rendering its output in a child window of the first process).

62. Regarding claim 69, Narin teaches wherein at least one corrupted file residing on the second memory space is capable of being deleted when the second browser process is terminated (Figure 4 [step 412], paragraph 0044).

63. Regarding claim 70, Narin teaches wherein the first browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second browser process (Abstract, paragraph 0035-0036, 0039, the first process's address space is inaccessible to the second process; provides defense against from the non-secure software object (i.e. web browsing functions, from observing or modifying anything going on with the secure application)).

64. Regarding claim 71, Narin teaches wherein attempts by malware to record data entry by a computer user are effectively blocked (paragraph 0035, provide defense against observation and/or modification).

***Claim Rejections - 35 USC § 103***

65. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Art Unit: 2439

66. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Narin.

67. Regarding claim 3, Narin does not teach wherein the first logical process is capable of accessing data contained in the second memory space.

68. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the first logical process to access data stored in the second memory space, since one of ordinary skill in the art would recognize that the first logical process of Narin is the master process (since it spawns the second process, see paragraphs 0037-0038, 0041-0042), which means it may need to access the second memory space in order to perform administrative functions with regards to the second process.

69. Claims 6, 20, 27, 28, 37, 38, 49, 50, and 68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narin in view of U.S. Patent No. 7,024,581 B1 to Wang et al., hereinafter Wang.

70. Regarding claims 6, 20, 27, 37, 49, and 68, Narin does not teach at least one corrupted file required for a browser process is capable of being restored from a protected image.

71. Wang teaches restoring at least one corrupted data file from a protected image (Figures 2 [elements 72, 74, 76, 78, 80, 82], 3 [element 140], 6 [element 236], 7 [element 272], column 9, lines 13-67).

72. It would have been obvious to one of ordinary skill in the art at the time the invention was made to restore at least one corrupted data file from a protected image, since Wang states at column 2, lines 49-60 that using a protected image takes advantage of today's computing power and storage capabilities to increase the reliability, accessibility, flexibility, and performance of computers and the backup/restore process.

Art Unit: 2439

73. With regards to claims 28, 38, and 50, Wang teaches wherein the protected image is stored at a location selected from the group consisting of: a removable drive; the first memory space; a partition on a memory device image (Figures 2 [elements 72, 74, 76, 78, 80, 82], 3 [element 140], 6 [element 236], 7 [element 272], column 9, lines 13-67); a nonvolatile memory disk; another device (Figure 4).

74. Claim 57 is rejected under 35 U.S.C. 103(a) as being unpatentable over Narin.

75. Regarding claim 57, Narin does not teach the first browser process opening a plurality of second browser processes.

76. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the first browser process to open a plurality of second browser processes, since one of ordinary skill in the art would recognize that web pages may have several processes from different service providers that could be regarded as nefarious, thereby having a need to generate a second process for each of the potentially nefarious processes. Furthermore, it has been held that merely duplicating a part or its function has no patentable significance unless it produces new and unexpected results. See MPEP § 2144.04(VI)(B).

#### ***Double Patenting***

77. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection

Art Unit: 2439

is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

78. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

79. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

80. Claims 21-73 are provisionally rejected on the ground of nonstatutory double patenting over claims 21-55 of copending Application No. 12/720,207. This is a provisional double patenting rejection since the conflicting claims have not yet been patented.

81. The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on that copending application

Art Unit: 2439

since the referenced copending application and the instant application are claiming common subject matter, and only differ in the type of device implementing the claimed invention.

*Allowable Subject Matter*

82. Claims 8, 9, 13, and 18 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Claims 8, 9, 13, and 18 would be allowable if the rejections set forth in this Office action were overcome and all of the limitations of the base claim and any intervening claims were included in those claims.

*Conclusion*

83. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

84. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

85. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

Art Unit: 2439

86. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

87. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/  
Primary Examiner, Art Unit 2439

clf

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	36	rozman-all\$.in.	US-PGPUB; USPAT	OR	OFF	2007/09/13 09:28
S2	2	cioffi-alf\$.in.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:49
S3	1	"6289462".pn.	US-PGPUB; USPAT	OR	OFF	2007/09/13 09:32
S4	10	((("7146640") or ("5835695") or ("6578140") or ("20050149933") or ("6892261") or ("6678712") or ("6957286") or ("6996828") or ("20040205755") or ("6697972")).PN.	US-PGPUB; USPAT	OR	OFF	2007/09/13 09:33
S5	5	("6578140").URPN.	USPAT	OR	OFF	2007/09/13 10:01
S6	1	(dual multiple) near (OS operat\$3 near systems) with (prevent\$3 stop\$4) with (virus trojan malicious malware)	US-PGPUB; USPAT	OR	ON	2007/09/13 10:06
S7	15	("6385721").URPN.	USPAT	OR	OFF	2007/09/13 10:03
S8	8	(dual multiple) near (OS operat\$3 near systems) with (virus trojan malicious malware)	US-PGPUB; USPAT	OR	ON	2007/09/13 13:58
S9	0	("2004/0039944").URPN.	USPAT	OR	OFF	2007/09/13 10:09
S10	35	((("5826013") or ("5978917") or ("6735700") or ("6663000") or ("6553377") or ("6216112") or ("4890098") or ("5555364") or ("5666030") or ("5995103") or ("5502808") or ("5280579") or ("5918039") or ("6480198") or	US-PGPUB; USPAT	OR	OFF	2007/09/13 10:13

		("6167522") or ("6199181") or ("6275938") or ("6351816") or ("6456554") or ("6658573") or ("6507904") or ("6633963") or ("6678825") or ("5751979") or ("20040054588") or ("20040034794") or ("20040006715") or ("20030177397") or ("20030097591") or ("20030023857") or ("20020066016") or ("20020174349") or ("6581162") or ("6134661") or ("6578140").PN.				
S11	8	(US-20040039944-\$).did. or (US-7146640-\$ or US- 6996828-\$ or US-6678712- \$ or US-6578140-\$ or US- 6385721-\$ or US-7260839- \$ or US-6199181-\$).did.	US-PGPUB; USPAT	OR	OFF	2007/09/13 10:28
S12	0	S11 and network\$3 near (OS operat\$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 10:29
S13	8565	network\$3 near (OS operat \$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 10:29
S14	2	(dual multiple) near (OS operat\$3 near systems) same (display\$3) with both with (OS\$2 operat\$3 near systems)	US-PGPUB; USPAT	OR	ON	2007/09/13 11:55
S15	67	(dual multiple) near (OS operat\$3 near systems) same (display\$3) with (multiple) with (OS\$2 operat\$3 near systems)	US-PGPUB; USPAT	OR	ON	2007/09/13 11:55
S16	41	("5673403").URPN.	USPAT	OR	OFF	2007/09/13 12:12
S17	4565	(dual multiple) near (OS operat\$3 near systems)	US-PGPUB; USPAT	OR	ON	2007/09/13 14:49
S18	688	multi\$score near (processor cpu)	US-PGPUB; USPAT	OR	ON	2007/09/13 13:59
S19	37	S17 and S18	US-PGPUB; USPAT	OR	ON	2007/09/13 13:59
S20	18	S17 same S18	US-PGPUB; USPAT	OR	ON	2007/09/13 14:00



S21	4	S17 with S18	US-PGPUB; USPAT	OR	ON	2007/09/13 13:59
S22	14	S17 same S18 not S21	US-PGPUB; USPAT	OR	ON	2007/09/13 14:01
S23	19	S19 not S20	US-PGPUB; USPAT	OR	ON	2007/09/13 14:01
S24	665	(dual multiple) near (OS operat\$3 near systems) and (remov\$3 delet\$3) with (file program)	US-PGPUB; USPAT	OR	ON	2007/09/13 14:50
S25	1	(dual multiple) near (OS operat\$3 near systems) and (remov\$3 delet\$3) with (file program) with after near (run\$3 ran execut\$3)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:09
S26	17	(dual multiple) near (OS operat\$3 near systems) with encrypt\$3 \	US-PGPUB; USPAT	OR	ON	2007/09/13 15:09
S27	17	(dual multiple) near (OS operat\$3 near systems) with encrypt\$3	US-PGPUB; USPAT	OR	ON	2007/09/13 15:19
S28	36	(dual multiple) near (OS operat\$3 near systems) same encrypt\$3	US-PGPUB; USPAT	OR	ON	2007/09/13 15:19
S29	19	(dual multiple) near (OS operat\$3 near systems) same encrypt\$3 not S27	US-PGPUB; USPAT	OR	ON	2007/09/13 15:23
S30	676	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 not S28	US-PGPUB; USPAT	OR	ON	2007/09/13 15:33
S31	12	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (inter \$OS inter\$operat\$3 near system inter\$process\$2)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:35
S32	0	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (data information) with first near (OS operat\$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:38
S33	1	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with first near (OS operat\$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:37

S34	9	(US-20040039944-\$).did. or (US-7146640-\$ or US- 6996828-\$ or US-6678712- \$ or US-6578140-\$ or US- 6385721-\$ or US-7260839- \$ or US-6199181-\$ or US- 5673403-\$).did.	US-PGPUB; USPAT	OR	OFF	2007/09/13 15:37
S35	2	S34 and encrypt\$3	US-PGPUB; USPAT	OR	ON	2007/09/13 15:37
S36	81	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (OS operat\$3 near system) with (transfer communicat\$3 data)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:39
S37	6	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (OS operat\$3 near system) with (transfer communicat\$3)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:39
S38	0	731/1.ccls.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:12
S39	2670	713/1.ccls.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:12
S40	1	"7027872".pn.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:52
S41	0	"7027872".pn. and IMD with (authentikat\$3 authori \$6 verif\$7 valid\$5)	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:52
S42	1	"7027872".pn. and (authentikat\$3 authori\$6 verif\$7 valid\$5)	US-PGPUB; USPAT	OR	OFF	2007/09/13 17:06
S43	1	"20050022020".pn.	US-PGPUB; USPAT	OR	OFF	2007/09/13 17:06
S44	1	"6192477".pn.	US-PGPUB; USPAT	OR	OFF	2008/02/19 13:13
S45	9	("6192477").URPN.	USPAT	OR	OFF	2008/02/19 13:14
S46	9	("6192477").URPN.	USPAT	OR	OFF	2008/06/16 16:15
S47	9	("6192477").URPN.	USPAT	OR	OFF	2008/06/16 16:15
S48	5	("6578140").URPN.	USPAT	OR	OFF	2008/08/18 14:31
S49	63	secure near3 process\$3 same insecure near3 process\$3	US-PGPUB; USPAT	OR	ON	2008/08/18 14:32

S50	1	secure near3 process\$3 same insecure near3 process\$3 with (internet e \$1mail)	US-PGPUB; USPAT	OR	ON	2008/08/18 14:32
S51	0	secure near3 processor and insecure near3 processor with (internet e \$1mail)	US-PGPUB; USPAT	OR	ON	2008/08/18 14:33
S52	9	("6192477").URPN.	USPAT	OR	OFF	2008/08/18 16:04
S53	1	common near (operat\$3 nears system OS) same protect\$3 near processor	US-PGPUB; USPAT	OR	ON	2008/08/18 16:33
S54	36	common near (operat\$3 nears system OS) and protect\$3 near processor	US-PGPUB; USPAT	OR	ON	2008/08/18 16:33
S55	0	(common near (operat\$3 nears system OS) and protect\$3 near processor). clm.	US-PGPUB; USPAT	OR	ON	2008/08/18 16:34
S56	1	"7484247".pn.	US-PGPUB; USPAT	OR	OFF	2010/12/21 13:22
S57	8	((("5673403") or ("5751979") or ("5974549") or ("5978917") or ("6091412") or ("6134661") or ("6397242") or ("6401134")).PN.	USPAT	OR	OFF	2010/12/21 13:27
S58	173	("5974549").URPN.	USPAT	OR	OFF	2010/12/21 13:29
S59	11	((("6433794") or ("6438600") or ("6492995") or ("6678825") or ("6691230") or ("6757685") or ("6836885") or ("7024555") or ("7139890") or ("7146640") or ("7260839")).PN.	USPAT	OR	OFF	2010/12/21 13:48
S60	3	((("7401230") or ("7421689") or ("7565522")).PN.	USPAT	OR	OFF	2010/12/21 13:51
S61	1291	eros	US-PGPUB; USPAT	OR	ON	2010/12/21 14:13
S62	12	eros and ("726" "713" "380").clas.	US-PGPUB; USPAT	OR	ON	2010/12/21 14:13

S63	0	eros with trust\$3 with window	US-PGPUB; USPAT	OR	ON	2010/12/21 14:14
S64	8	((("4890098") or ("5280579") or ("5502808") or ("5555364") or ("5666030") or ("5673403") or ("5751979") or ("5826013"))).PN.	USPAT	OR	OFF	2010/12/21 14:54
S65	11	((("5918039") or ("5978917") or ("5995103") or ("6134661") or ("6167522") or ("6192477") or ("6199181") or ("6216112") or ("6275938") or ("6351816") or ("6385721"))).PN.	USPAT	OR	OFF	2010/12/21 14:56
S66	11	((("6480198") or ("6507904") or ("6507948") or ("6546554") or ("6553377") or ("6578140") or ("6581162") or ("6633963") or ("6658573") or ("6663000") or ("6678825"))).PN.	USPAT	OR	OFF	2010/12/21 14:58
S67	65	("6678825").URPN.	USPAT	OR	OFF	2010/12/21 14:58
S68	8	("6578140").URPN.	USPAT	OR	OFF	2010/12/21 15:09
S69	4	((("6735700") or ("6321337") or ("7146640") or ("7260839"))).PN.	USPAT	OR	OFF	2010/12/21 15:10
S70	5	((("20020066016") or ("20020174349") or ("20030023857") or ("20030097591") or ("20030177397"))).PN.	US-PGPUB	OR	OFF	2010/12/21 15:12
S71	6	((("20040006715") or ("20040034794") or ("20040039944") or ("20040054588") or ("20050240810") or ("20060004667"))).PN.	US-PGPUB	OR	OFF	2010/12/21 15:13

S72	8	(("6880110") or ("7096381") or ("7577871") or ("7694328") or ("7373505") or ("7039801") or ("7596694") or ("7085928")).PN.	USPAT	OR	OFF	2010/12/21 15:18
S73	11	(("7181768") or ("7284274") or ("6804780") or ("7191469") or ("6505300") or ("7246374") or ("7062672") or ("7444412") or ("6772345") or ("6108715") or ("6873988")).PN.	USPAT	OR	OFF	2010/12/21 15:21
S74	1	"20030131152".pn.	US-PGPUB; USPAT	OR	OFF	2010/12/21 15:23
S75	4522	janus	US-PGPUB; USPAT	OR	OFF	2010/12/21 15:24
S76	1	"7484247".pn.	US-PGPUB; USPAT	OR	OFF	2010/12/21 15:47
S77	0	("7818808").URPN.	USPAT	OR	OFF	2010/12/22 06:08
S78	38	(execut\$3 run\$4) with (web HTML XML content) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:10
S79	2	(execut\$3 run\$4) with (plug \$in applet java\$script embed\$4 near executable) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:15
S80	2	(execut\$3 run\$4 render\$3) with (plug\$in applet java \$script embed\$4 near executable) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:15
S81	4	(execut\$3 run\$4 render\$3) with (malicious virus malware trojan spyware adware) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:17
S82	3	("2005/0005153").URPN.	USPAT	OR	OFF	2010/12/22 06:20

S83	2	(execut\$3 run\$4) with (plug \$in applet java\$script embed\$4 near (content executable)) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:21
S84	0	(execut\$3 run\$4 render\$3) with (separate isolat\$3) near (CPU processor microprocessor) same (detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:21
S85	70	(execut\$3 run\$4 render\$3) with (separate isolat\$3) near (CPU processor microprocessor) and (detect \$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:21
S86	35	sandbox\$3 with (CPU processor microprocessor) same (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:29
S87	15	sandbox\$3 with (CPU processor microprocessor) and (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) not S86	US-PGPUB; USPAT	OR	ON	2010/12/22 06:30
S88	9	("20050283836" "20030051027" "20060259948" "20060191008" "20060080735" "6785732" "20050131868" "20010032205" "20060101514").pn.	US-PGPUB; USPAT	OR	ON	2010/12/22 06:33
S89	4	(web internet embed\$4) near (video audio content media) with (CPU processor microprocessor) same (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:37
S90	54	("5751979").URPN.	USPAT	OR	OFF	2010/12/22 06:39

S91	67	(web internet embed\$4) near (video audio content media) with (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:41
S92	3	(separate isolat\$3) near (CPU processor microprocessor) with (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:47
S93	5	(execut\$3 run\$4 render\$3) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:56
S94	0	((web internet embed\$4) near (content media video audio page site) web\$site web\$page) with (separate isolat\$3) near (CPU processor microprocessor) same (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:57
S95	3	(separate isolat\$3) near (CPU processor microprocessor) with (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:57
S96	1181	(CPU processor microprocessor) with (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:58

S97	15	(CPU processor microprocessor) with (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware) with ((web internet embed\$4) near (content media video audio page site) web\$site web \$page)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:58
S98	15	(CPU processor microprocessor) with (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware) with ((web internet embed\$4) near (content media video audio page site) web\$site web \$page) not S87	US-PGPUB; USPAT	OR	ON	2010/12/22 06:59
S99	0	(separate special\$4 isolat \$3 individual\$4) with (CPU processor microprocessor) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin \$5 check\$3) with (malicious virus malware trojan spyware adware) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page) not S87	US-PGPUB; USPAT	OR	ON	2010/12/22 07:03
S100	0	(separate special\$4 isolat \$3 individual\$4) with (CPU processor microprocessor) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page) same (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3 prevent\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:03



S101	31	(CPU processor microprocessor) with ((web internet embed\$4) near (content media video audio page site) web\$site web \$page) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3 prevent\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:04
S102	0	(execut\$3 run\$4 render\$3) with (separate isolat\$3) near (CPU processor microprocessor) with sandbox\$3	US-PGPUB; USPAT	OR	ON	2010/12/22 07:11
S103	0	(separate isolat\$3) near (CPU processor microprocessor) with sandbox\$3	US-PGPUB; USPAT	OR	ON	2010/12/22 07:11
S104	36	(CPU processor microprocessor) with sandbox\$3 with (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3 prevent\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:11
S105	11	(("20050198692") or ("20050234856") or ("20060242166") or ("20060242709") or ("20060271835") or ("20080184105") or ("20080178302") or ("20080263358") or ("7562293") or ("7607172") or ("7698559")).PN.	US-PGPUB; USPAT	OR	OFF	2010/12/22 07:14
S106	2	("2005/0198692").URPN.	USPAT	OR	OFF	2010/12/22 07:21
S107	8	("20050198692"   "5832208"   "6092194"   "6240530"   "6675174"   "6701440"   "7171691"   "7263561").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2010/12/22 07:22
S108	54	("5751979").URPN.	USPAT	OR	OFF	2010/12/22 07:24

S109	0	(divid\$3 division split\$4 spread\$3) with (CPU processor microprocessor) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page) same (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:41
S110	7	(divid\$3 division split\$4 spread\$3) with (CPU processor microprocessor) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page) and (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:42
S111	183	(divid\$3 division split\$4 spread\$3) with (CPU processor microprocessor) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:43
S112	61	(execut\$3 run\$4 render\$3 display\$3 reproduc\$3) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page plug\$in script java\$script perl\$script) with (separate isolat\$3 individual second other) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 11:02
S113	9	(execut\$3 run\$4 render\$3 display\$3 reproduc\$3) with (suspicious malicious malware suspect\$2) with (separate isolat\$3 individual second other) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 14:18

S114	68	(execut\$3 run\$4 render\$3 display\$3 reproduc\$3) with (download\$2) with (separate isolat\$3 individual second other) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 14:20
S115	178	("5974549").URPN.	USPAT	OR	OFF	2010/12/28 14:11
S116	1	(CPU processor micro \$processor) with delegat\$3 same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin \$5 check\$3) with (malicious virus malware trojan spyware adware)	USPAT	OR	ON	2010/12/28 14:16
S117	7	(CPU processor micro \$processor) with delegat\$3 and (protect\$3 secur\$3 safe \$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check \$3) with (malicious virus malware trojan spyware adware)	USPAT	OR	ON	2010/12/28 14:17
S118	8	(CPU processor micro \$processor) with (transfer \$4 delegat\$3 assign\$4) with (task process application) same (protect \$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	USPAT	OR	ON	2010/12/28 14:18
S119	19	("6678712").URPN.	USPAT	OR	OFF	2010/12/28 14:21
S120	8	("6578140").URPN.	USPAT	OR	OFF	2010/12/28 14:27
S121	5	("20060107055"   "20080301670"   "6016546"   "6195587"   "6578140").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2010/12/28 14:27
S122	56	(virus anti\$virus) near (processor co\$processor)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:31

S123	3738	(CPU processor micro \$processor co\$processor video adj processor) with (display\$3 render\$3 reproduc\$4) with ((web internet embed\$4) near (content media video audio page site) web\$site web \$page)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:34
S124	1	(CPU processor micro \$processor co\$processor video adj processor) with (display\$3 render\$3 reproduc\$4) with ((web internet embed\$4) near (content media video audio page site) web\$site web \$page) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:35
S125	14	(CPU processor micro \$processor co\$processor video adj processor) with (display\$3 render\$3 reproduc\$4) with ((web internet embed\$4) near (content media video audio page site) web\$site web \$page) and (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) with ((web internet embed \$4) near (content media video audio page site) web \$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:35
S126	95	("6199181").URPN.	USPAT	OR	OFF	2010/12/28 14:38
S127	2	("2004/0039944").URPN.	USPAT	OR	OFF	2010/12/28 14:47
S128	14	("6192477").URPN.	USPAT	OR	OFF	2010/12/28 14:48
S129	1	"7146305".pn.	USPAT	OR	OFF	2010/12/28 14:50

SI30	235	("20010034847"   "20020032717"   "20020032793"   "20020032880"   "20020035698"   "20020083331"   "20020083334"   "20020138753"   "20020144156"   "20030037136"   "20030088791"   "20030212903"   "20040010718"   "4223380"   "4400769"   "4672609"   "4773028"   "4819234"   "4975950"   "5032979"   "5121345"   "5204966"   "5210704"   "5274824"   "5278901"   "5309562"   "5311593"   "5345595"   "5347450"   "5353393"   "5359659"   "5371852"   "5398196"   "5414833"   "5440723"   "5452442"   "5454074"   "5475839"   "5511184"   "5515508"   "5522026"   "5539659"   "5557742"   "5586260"   "5590331"   "5606668"   "5623600"   "5623601"   "5630061"   "5649095"   "5649185"   "5675711"   "5696486"   "5696822"   "5706210"   "5734697"   "5745692"   "5748098"   "5761504"   "5764887"   "5764890"   "5765030"   "5774727"   "5787177"   "5790799"   "5796942"   "5798706"   "5812763"   "5815574"   "5822517"   "5826013"   "5828833"   "5832208"   "5832211"   "5835726"   "5838903"   "5842002"   "5845067"   "5848233"   "5854916"   "5857191"   "5864665"   "5864803"   "5872978"   "5875296"   "5878420"   "5881236"   "5884033"   "5892903"   "5899999"   "5907834"   "5919257"   "5919258"   "5922051"   "5925126"   "5931946"   "5940591"   "5950012"   "5961644"	US-PGPUB; USPAT; USOCR	OR	OFF	2010/12/28 14:50
------	-----	---	------------------------------	----	-----	---------------------

"5964839"	"5964889"
"5974237"	"5974457"
"5978917"	"5983270"
"5983348"	"5983350"
"5987606"	"5987610"
"5987611"	"5991856"
"5991881"	"5999711"
"5999723"	"6003132"
"6006016"	"6009467"
"6014645"	"6016553"
"6021510"	PN. OR
("6026442"	"6029256"
"6035323"	"6035423"
"6041347"	"6052709"
"6061795"	"6067410"
"6070190"	"6070244"
"6073172"	"6081894"
"6085224"	"6088803"
"6088804"	"6092194"
"6094731"	"6098173"
"6104783"	"6108799"
"6118940"	"6119165"
"6119234"	"6122738"
"6144961"	"6154844"
"6161109"	"6167520"
"6173413"	"6185689"
"6195687"	"6199181"
"6205552"	"6226372"
"6230288"	"6266773"
"6266774"	"6271840"
"6272641"	"6275938"
"6275942"	"6278886"
"6279113"	"6282546"
"6298445"	"6301668"
"6314520"	"6314525"
"6321338"	"6324627"
"6324647"	"6324656"
"6338141"	"6347374"
"6353385"	"6357008"
"6377994"	"6396845"
"6397242"	"6397245"
"6405318"	"6405364"
"6408391"	"6415321"
"6429952"	"6434615"
"6438600"	"6445822"
"6453345"	"6453346"
"6460141"	"6463426"
"6470449"	"6477585"
"6477648"	"6477651"
"6484203"	"6487666"
"6496858"	"6499107"
"6510523"	"6517587"
"6519647"	"6519703"
"6530024"	"6535227"
"6546493"	"6563959"
"6574737"	"6578147"
"6584454"	"6601190"

		"6606744"   "6618501"   "6628824"   "6647139"   "6647400"   "6661904"   "6668082"   "6668084"   "6681331"   "6691232"   "6704874"   "6708212"   "6711127"   "6711615"   "6718383"   "6721806"   "6725377"   "6725378"   "6775780"   "6792144"   "6792546"   "6816973"   "6839850"   "6851057"). PN.				
S131	12	("7146305").URPN.	USPAT	OR	OFF	2010/12/28 14:51
S132	5	restor\$3 with (file application program) with protect\$3 near image	US-PGPUB; USPAT	OR	ON	2010/12/28 17:07
S133	49	sub\$operat\$3 near system	US-PGPUB; USPAT	OR	ON	2010/12/29 15:43
S134	4503	(secure protect\$3 sand\$box \$3) with (web internet) near (browser viewer application)	US-PGPUB; USPAT	OR	ON	2010/12/30 11:06
S135	4100	(secure protect\$3 sand\$box \$3) with (web internet) adj (browser viewer application)	US-PGPUB; USPAT	OR	ON	2010/12/30 11:06
S136	4073	(secure protect\$3) with (web internet) adj (browser viewer application)	US-PGPUB; USPAT	OR	ON	2010/12/30 11:07
S137	15	(secure protect\$3) with (web internet) adj (browser viewer application) same sand\$box \$3 with (content media video audio embed\$4)	US-PGPUB; USPAT	OR	ON	2010/12/30 11:07
S138	19	(secure protect\$3) with (web internet) adj (browser viewer application) and sand\$box \$3 with (content media video audio embed\$4) not S137	US-PGPUB; USPAT	OR	ON	2010/12/30 11:09
S139	1	(US-20050149726-\$.)did.	US-PGPUB	OR	OFF	2010/12/30 11:30
S140	1	S139 and scan\$4	US-PGPUB; USPAT	OR	ON	2010/12/30 11:30
S141	55	("2005/0149726").URPN.	USPAT	OR	OFF	2010/12/30 11:33

S142	0	S139 and (permission permitting permit)	USPAT	OR	ON	2010/12/30 11:40
S143	2	(US-20050149726-\$).did. or (US-7146305-\$).did.	US-PGPUB; USPAT	OR	OFF	2010/12/30 12:18
S144	2	S143 and (cell\$4 mobile)	US-PGPUB; USPAT	OR	ON	2010/12/30 12:19
S145	258	list\$3 with block\$3 with (web\$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/30 12:24
S146	2	list\$3 with block\$3 with (web\$site web\$page) with (virus malware infection malicious trojan worm)	US-PGPUB; USPAT	OR	ON	2010/12/30 12:24
S147	4	list\$3 with block\$3 with (web\$site web\$page) same (virus malware infection malicious trojan worm)	US-PGPUB; USPAT	OR	ON	2010/12/30 12:25
S148	3	list\$3 with block\$3 with (web\$site web\$page) and 726/22-24.ccls.	US-PGPUB; USPAT	OR	ON	2010/12/30 12:25
S149	19	list\$3 with block\$3 with (web\$site web\$page) and "726".clas.	US-PGPUB; USPAT	OR	ON	2010/12/30 12:26
S150	10	(list\$3 with block\$3 black \$list\$3) with (web\$site web \$page) with (virus malware infection malicious trojan worm)	US-PGPUB; USPAT	OR	ON	2010/12/30 12:27
S151	16	(list\$3 with block\$3 black \$list\$3) with (web\$site web \$page) same (virus malware infection malicious trojan worm)	US-PGPUB; USPAT	OR	ON	2010/12/30 12:27
S152	6	(list\$3 with block\$3 black \$list\$3) with (web\$site web \$page) same (virus malware infection malicious trojan worm) not S150	US-PGPUB; USPAT	OR	ON	2010/12/30 12:27
S153	10	(list\$3 with block\$3 black \$list\$3) with (web\$site web \$page) and 726/22-24.ccls.	US-PGPUB; USPAT	OR	ON	2010/12/30 12:29
S154	7	(list\$3 with block\$3 black \$list\$3) with (web\$site web \$page) and 726/22-24.ccls. not S150	US-PGPUB; USPAT	OR	ON	2010/12/30 12:29
S155	10	(list\$3 with block\$3 black \$list\$3) with (web\$site web \$page) with (virus malware infect\$3 malicious trojan worm)	US-PGPUB; USPAT	OR	ON	2010/12/30 12:29



S156	43	(list\$3 with block\$3 black \$list\$3) with (web\$site web \$page) and ("726" "713"). clas.	US-PGPUB; USPAT	OR	ON	2010/12/30 12:30
S157	34	(list\$3 with block\$3 black \$list\$3) with (web\$page web\$site site page) with (malicious malware infect \$3 virus) and ("726" "713"). clas.	US-PGPUB; USPAT	OR	ON	2010/12/30 12:32
S158	37	((list\$3 table data\$base) with block\$3 black\$list\$3) with (web\$page web\$site site page) with (malicious malware infect\$3 virus) and ("726" "713").clas.	US-PGPUB; USPAT	OR	ON	2010/12/30 12:34
S159	3	((list\$3 table data\$base) with block\$3 black\$list\$3) with (web\$page web\$site site page) with (malicious malware infect\$3 virus) and ("726" "713").clas. not S157	US-PGPUB; USPAT	OR	ON	2010/12/30 12:34
S160	1	(US-7484247-\$).did.	USPAT	OR	OFF	2010/12/30 15:05
S161	1	"20040267929".pn.	US-PGPUB; USPAT	OR	OFF	2010/12/30 15:06
S162	1	(US-7484247-\$).did. and search\$3 near request\$3	USPAT	OR	ON	2010/12/30 15:06
S163	0	(secure protect\$3) with (web internet) adj (browser viewer application) same (prevent \$3 stop\$4) with search\$3 with (hack malicious\$2 hi \$jack)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:15
S164	1	(secure protect\$3) with (web internet) adj (browser viewer application) and (prevent \$3 stop\$4) with search\$3 with (hack malicious\$2 hi \$jack)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:15
S165	36	(prevent\$3 stop\$4) with search\$3 with (hack malicious\$2 hi\$jack)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:16
S166	58	search\$3 near (engine request) near4 (hack malicious\$2 hi\$jack)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:18
S167	59	search\$3 near (engine request) near4 (hack malicious\$2 hi\$jack\$3)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:19

S168	1	search\$3 near (engine request) near4 (hack malicious\$2 hi\$jack\$3) not S166	US-PGPUB; USPAT	OR	ON	2010/12/30 15:19
S169	3728010	prevent\$3 search\$3 near4 (hack malicious\$2 hi\$jack \$3)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:21
S170	15	prevent\$3 with search\$3 near4 (hack malicious\$2 hi \$jack\$3)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:21
S171	59	("2005/0149726").URPN.	USPAT	OR	OFF	2011/03/03 16:07
S172	59	("2005/0149726").URPN.	USPAT	OR	OFF	2011/03/03 16:07
S173	2915	726/23-24.ccls.	US-PGPUB; USPAT	OR	OFF	2011/04/12 12:48
S174	5374	709/225.ccls.	US-PGPUB; USPAT	OR	OFF	2011/04/12 12:48
S175	93	S173 and S174	US-PGPUB; USPAT	OR	OFF	2011/04/12 12:48
S176	2	S173 and S174 and secure with browser	US-PGPUB; USPAT	OR	ON	2011/04/12 12:49
S177	911	713/151.ccls.	US-PGPUB; USPAT	OR	ON	2011/04/12 12:50
S178	422	713/152.ccls.	US-PGPUB; USPAT	OR	ON	2011/04/12 12:50
S179	25	S178 and S173	US-PGPUB; USPAT	OR	ON	2011/04/12 12:50
S180	1	"7039801".pn.	US-PGPUB; USPAT	OR	OFF	2011/04/12 12:59
S181	4	("7039801").URPN.	USPAT	OR	OFF	2011/04/12 13:38
S182	1	"20020002673".pn.	US-PGPUB; USPAT	OR	OFF	2011/04/12 13:38
S183	5	("6049838"   "6108715"   "6330670"   "6434679"   "6487665").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2011/04/12 13:39
S184	10	("2002/0002673").URPN.	USPAT	OR	OFF	2011/04/12 13:40
S185	0	(block\$3 with modif\$7 with search near request\$3).clm.	US-PGPUB; USPAT	OR	ON	2011/04/12 13:51
S187	1	(US-7484247-\$).did.	USPAT	OR	OFF	2011/10/19 12:08
S188	1	S187 and browser	US-PGPUB; USPAT	OR	ON	2011/10/19 12:08

S189	5	((("6183366") or ("6285987") or ("20040199763") or ("6990630") or ("7676842"))).PN.	US-PGPUB; USPAT	OR	OFF	2011/10/19 14:30
------	---	---	-----------------	----	-----	---------------------

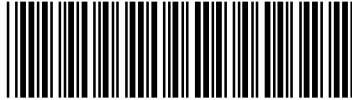
### EAST Search History (I nterference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S186	0	(block\$3 with modif\$7 with search near request \$3).clm.	USPAT; UPAD	OR	ON	2011/04/12 13:51

10/ 25/ 11 2:27:28 PM

C:\ Documents and Settings\ claforgia\ My Documents\ EAST\ Workspaces\ 12720147.wsp



<b>Index of Claims</b>  	<b>Application/Control No.</b> 12720147	<b>Applicant(s)/Patent Under Reexamination</b> ROZMAN ET AL.
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439

✓	<b>Rejected</b>
=	<b>Allowed</b>

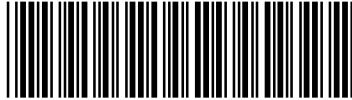
-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/29/2010	04/25/2011	10/20/2011					
	1	✓	✓	✓					
	2	✓	✓	✓					
	3	✓	✓	✓					
	4	✓	✓	✓					
	5	✓	✓	✓					
	6	✓	✓	✓					
	7	✓	✓	✓					
	8	✓	✓	✓					
	9	✓	✓	✓					
	10	✓	✓	✓					
	11	✓	✓	✓					
	12	✓	✓	✓					
	13	✓	✓	✓					
	14	✓	✓	✓					
	15	✓	✓	✓					
	16	✓	✓	✓					
	17	✓	✓	✓					
	18	✓	✓	✓					
	19	✓	✓	✓					
	20	✓	✓	✓					
	21	✓	✓	✓					
	22	✓	✓	✓					
	23	✓	✓	✓					
	24	✓	✓	✓					
	25	✓	✓	✓					
	26	✓	✓	✓					
	27	✓	✓	✓					
	28	✓	✓	✓					
	29	✓	✓	✓					
	30	✓	✓	✓					
	31	✓	✓	✓					
	32	✓	✓	✓					
	33	✓	✓	✓					
	34	✓	✓	✓					
	35	✓	✓	✓					
	36	✓	✓	✓					

<b>Index of Claims</b>  	<b>Application/Control No.</b> 12720147	<b>Applicant(s)/Patent Under Reexamination</b> ROZMAN ET AL.
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439

✓	<b>Rejected</b>
=	<b>Allowed</b>

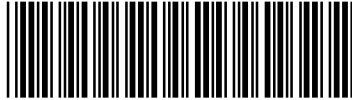
-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/29/2010	04/25/2011	10/20/2011					
	37	✓	✓	✓					
	38	✓	✓	✓					
	39	✓	✓	✓					
	40	✓	✓	✓					
	41	✓	✓	✓					
	42	✓	✓	✓					
	43	✓	✓	✓					
	44	✓	✓	✓					
	45	✓	✓	✓					
	46	✓	✓	✓					
	47	✓	✓	✓					
	48	✓	✓	✓					
	49	✓	✓	✓					
	50	✓	✓	✓					
	51	✓	✓	✓					
	52	✓	✓	✓					
	53	✓	✓	✓					
	54	✓	✓	✓					
	55	✓	✓	✓					
	56	✓	✓	✓					
	57	✓	✓	✓					
	58		✓	✓					
	59		✓	✓					
	60		✓	✓					
	61		✓	✓					
	62		✓	✓					
	63		✓	✓					
	64		✓	✓					
	65		✓	✓					
	66		✓	✓					
	67		✓	✓					
	68		✓	✓					
	69		✓	✓					
	70		✓	✓					
	71		✓	✓					
	72		✓	✓					

<b><i>Index of Claims</i></b>  	<b>Application/Control No.</b> 12720147	<b>Applicant(s)/Patent Under Reexamination</b> ROZMAN ET AL.
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/29/2010	04/25/2011	10/20/2011					
	73		✓	✓					

<b>Search Notes</b>  	<b>Application/Control No.</b>  12720147	<b>Applicant(s)/Patent Under Reexamination</b>  ROZMAN ET AL.
	<b>Examiner</b>  Christian LaForgia	<b>Art Unit</b>  2439

SEARCHED			
Class	Subclass	Date	Examiner
none	none	12/29/10	clf
726	23-24	4/25/11	clf
713	152	4/25/11	clf
709	225	4/25/11	clf
none	none	10/19/11	clf

SEARCH NOTES		
Search Notes	Date	Examiner
updated search for 10/913,609 (USPN 7,484,247)	12/29/10	clf
updated EAST - see enclosed	4/25/11	clf
updated EAST - see enclosed	10/19/11	clf

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

	/Christian LaForgia/ Primary Examiner. Art Unit 2439
--	---





## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	12720147
<b>Filing Date:</b>	09-Mar-2010
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Filer:</b>	Glenn W. Boisbrun/Sherry Colgrove
<b>Attorney Docket Number:</b>	ARAC-01RE1

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
Request for continued examination	2801	1	465	465
Statutory or terminal disclaimer	2814	1	80	80
<b>Total in USD (\$)</b>				<b>545</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	11911492
<b>Application Number:</b>	12720147
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	8473
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Customer Number:</b>	25962
<b>Filer:</b>	Glenn W. Boisbrun/Sherry Colgrove
<b>Filer Authorized By:</b>	Glenn W. Boisbrun
<b>Attorney Docket Number:</b>	ARAC-01RE1
<b>Receipt Date:</b>	24-JAN-2012
<b>Filing Date:</b>	09-MAR-2010
<b>Time Stamp:</b>	18:21:55
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$545
RAM confirmation Number	18571
Deposit Account	501065
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	ARAC-01RE1_RCE.pdf	32856 cdd3d89be17e56dbfb062eb893566cc356e584fb	no	1

**Warnings:**

This is not a USPTO supplied RCE SB30 form.

**Information:**

2	Terminal Disclaimer Filed	ARAC-01RE1_Terminal_Disclaimer.pdf	24218 c91d13899bb15272d9bb414f7c71e699c8843c24	no	1
---	---------------------------	------------------------------------	---	----	---

**Warnings:**

**Information:**

3		ARAC-01RE1_Amendment_RCE.pdf	155420 4f54bc27cfa36a65f905840a880f9d787cab9982	yes	44
---	--	------------------------------	--	-----	----

**Multipart Description/PDF files in .zip description**

Document Description	Start	End
Amendment Submitted/Entered with Filing of CPA/RCE	1	1
Specification	2	2
Claims	3	19
Applicant Arguments/Remarks Made in an Amendment	20	44

**Warnings:**

**Information:**

4	Transmittal Letter	ARAC-01RE1_IDS_Transmittal.pdf	16611 7dde5a1458f70de309e5fdbb970ee79dc3680cac	no	1
---	--------------------	--------------------------------	---	----	---

**Warnings:**

**Information:**

5	Information Disclosure Statement (IDS) Form (SB08)	ARAC-01RE1_IDS.pdf	71892 988a657117c54c096772fa7ba002b7acfc444088	no	1
---	--	--------------------	---	----	---

**Warnings:**

**Information:**

This is not an USPTO supplied IDS fillable form

6	Fee Worksheet (SB06)	fee-info.pdf	32114 10b770100a40dc30b251764a0377e22915a d806d	no	2
---	----------------------	--------------	---	----	---

**Warnings:**

**Information:**

<b>Total Files Size (in bytes):</b>	333111
-------------------------------------	--------

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING  
REJECTION OVER A PENDING "REFERENCE" APPLICATION**Docket Number (Optional)  
ARAC-01RE1In re Application of: Rozman, *et al.*

Application No.: 12/720,147

Filed: March 9, 2010

For: System and Method for Protecting a Computer System from Malicious Software

The owner\*, Rozman & Cioffi, of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending **reference** Application Number 12/720,207, filed on March 9, 2010, as such term is defined in 35 U.S.C. 154 and 173, and as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the **reference** application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of any patent granted on said **reference** application, "as the term of any patent granted on said **reference** application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending **reference** application," in the event that: any such patent: granted on the pending **reference** application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

Check either box 1 or 2 below, if appropriate.

1.  For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2.  The undersigned is an attorney or agent of record. Reg. No. 39,615

/Glenn W. Boisbrun/ January 24, 2012  
Signature Date  
Glenn W. Boisbrun  
Typed or printed name  
972-732-1001  
Telephone Number

- Terminal disclaimer fee under 37 CFR 1.20 (d) is included.

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

\*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).

Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicants: Rozman, *et al.*                      Docket No.: ARAC-01RE1  
Serial No.: 12/720,147                              Filed: 03/09/2010  
Reissue of: 7,484,247                                Issued: January 27, 2009  
Title: System and Method for Protecting a Computer System from Malicious Software

Commissioner for Patents  
P. O. Box 1450  
Alexandria, VA 22313-1450

**AMENDMENT ACCOMPANYING RCE**

Dear Sir:

The Applicants respectfully submit the following amendments and remarks in response to Examiner's Office Action dated November 14, 2011, which Action is made final. This amendment accompanies a Request for Continued Examination. Favorable response is respectfully requested.



IN THE SPECIFICATION:

Before the heading “Cross Reference to Related Patents and Applications” kindly insert:

Cross Reference to Multiple Reissue Applications

This application is a reissue application of U.S. Patent No. 7,484,247, entitled “System and Method for Protecting a Computer System from Malicious Software,” issued on January 27, 2009, and is related to another reissue application designated U.S. Patent Application Serial No. 12/720,207 from U.S. Patent No. 7,484,247 filed concurrently herewith, which are incorporated herein by reference. This application is also related to another reissue application designated U.S. Patent Application Serial No. 12/854,149 (now, U.S. Patent No. RE43,103) from U.S. Patent No. 7,484,247 filed on August 10, 2010 and a continuation application therefrom designated U.S. Patent Application Serial No. 13/015,186 filed on January 27, 2011, which are incorporated herein by reference. This application is also related to another reissue application designated U.S. Patent Application Serial No. 12/941,067 from U.S. Patent No. 7,484,247 filed on November 7, 2010, which is incorporated herein by reference.

IN THE CLAIMS:

1. (Four Times Amended) A method of operating a computer system capable of exchanging data across a network of one or more computers and having at least a first and second electronic data processor capable of executing instructions using a common operating system, comprising[ the steps of]:

executing a first web browser process~~instructions~~, capable of accessing data of a website via the network, in a first logical process within the common operating system using the first electronic data processor, wherein the first logical process is capable of accessing data contained in a first memory space[ and a second memory space];

executing a second web browser process~~instructions~~ in a second logical process within the common operating system using the second electronic data processor, wherein the second logical process is capable of accessing data contained in the second memory space[, the second logical process being further capable of exchanging data across a network of one or more computers]; and

displaying[, in a windowed format on a display terminal,] data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to [the]a display[ terminal];

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser~~logical~~ process.

2. (Twice Amended) The method of claim 1 wherein the [ first memory space and the] second memory space [comprise separate regions of a common memory space is]comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

3. (Twice Amended) The method of claim 1 wherein the first logical process is capable of accessing data contained in the second memory spaces~~second logical process is selected from the group consisting of:~~

~~———— an electronic mail process, an instant messaging process, an internet browser process, an interactive gaming process, a virtual private network (VPN) process, and a reader application process.~~

4. (Original) The method of claim 1 wherein the first logical process receives user interface data, and passes the user interface data to the second logical process.

5. (Original) The method of claim 1 wherein the first and second electronic data processors are part of a multi-core electronic data processor.

6. (Twice Amended) The method of claim 1 and further comprising[ the step of] restoring at least one corrupted data file[ residing on the second memory space] from [an]a protected image[ residing on the first memory space].

7. (Amended) The method of claim 1 and further comprising[ the step of] automatically deleting at least one data file residing on the second memory space when the second logical process is terminated.

8. (Amended) The method of claim 1 and further comprising[ the steps of]:  
encrypting data with the first logical process;  
transferring the encrypted data from the first logical process to the second logical  
process; and  
transferring the encrypted data from the second logical process to the network interface  
device.

9. (Amended) The method of claim 8 and further comprising[ the steps of]:  
decrypting the data with the network interface device; and  
transferring the decrypted data from the network interface device to the network.

10. (Four Times Amended) A multi-processor computer system using a common  
operating system capable of exchanging data across a network of one or more computers via a  
network interface device, comprising:

a first electronic data processor capable of executing a first web browser  
process~~instructions~~ using the common operating system and communicatively coupled to a first  
memory space[ and a second memory space], the first web browser process capable of accessing  
data of a website via the network;

a second electronic data processor capable of executing a second web browser  
process~~instructions~~ using the common operating system and communicatively coupled to [the]a  
second memory space[ and a network interface device, wherein the second electronic data  
processor is capable of exchanging data across a network of one or more computers via the  
network interface device]; and

a video processor adapted to combine video data from the first and second electronic data  
processors and transmit the combined video data to a display[ terminal for displaying the

combines video data in a windowed format];

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser process on the second electronic data processor.

11. (Twice Amended) The computer system of claim 10 wherein the [ first memory space and the] second memory space [ comprise separate regions of a common memory space is] comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

12. (Original) The computer system of claim 10 wherein the first and second electronic data processors are part of a dual processor computer system.

13. (Original) The computer system of claim 10 wherein the second electronic data processor and the video processor are co-located on a circuit card, the circuit card being communicatively coupled to the first electronic data processor.

14. (Original) The computer system of claim 10 wherein the computer system is configured such that the first electronic data processor is protected from executing instructions initiated by a malware process downloaded from the network and executing on the second electronic data processor.

15. (Four Times Amended) A multi-processor computer system using a common operating system capable of exchanging data across a network of one or more computers,

comprising:

at least a first and second electronic data processor capable of executing instructions using the common operating system;

at least a first and second memory space; and

a video processor;

wherein the first and second electronic data processors, first and second memory space, and video processor are configured to:[for performing the steps of:]

[executing]execute a first web browser processinstructions, capable of accessing data of a website via the network, in a first logical process with the first electronic data processor, wherein the first logical process is executing within the common operating system and is capable of accessing data contained in the first memory space;

[executing]execute a second web browser processinstructions in a second logical process with the second electronic data processor, wherein the second logical process is executing within the common operating system and is capable of accessing data contained in the second memory space[, the second logical process being further capable of exchanging data across a network of one or more computers]; and

[displaying, in a windowed format on a display terminal,]display data from the first logical process and the second logical process, wherein the video processor is adapted to combine data from the first and second logical processes and transmit the combined data to [the]a display[ terminal];

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from

corruption by a malware process downloaded from the network and executing as part of the second web browser logical process.

16. (Original) The computer system of claim 15 wherein the computer system is further configured such that the first logical process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second logical process.

17. (Twice Amended) The computer system of claim 15 and further comprising[:] at least one network interface device capable of exchanging data with[ both the second logical process and with] the network and with a logical process that comprises a process selected from the group consisting of:

the first logical process; and

the second logical process.

18. (Original) The computer system of claim 17 wherein the network interface device is capable of decrypting data received from the second logical process and transmitting the decrypted data to the network while preventing the second logical process from accessing the decrypted data.

19. (Amended) The computer system of claim 15 wherein the at least one electronic data processor [is]comprises a processor selected from the group consisting of[:] a multi-core electronic data processor; dual electronic data processors; and multiple electronic data processors.

20. (Twice Amended) The computer system of claim 15 and further configured to restore[for performing the step of: restoring] at least one corrupted data file[ residing on the second memory space] from [an]a protected image[ residing on the first memory space].

21. (New) A portable computer capable of executing instructions using a common operating system, comprising:

a network interface device configured to exchange data across a network of one or more computers and access at least one website;

at least a first memory space and a second memory space, the first memory space containing at least one system file;

at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, wherein the user interface is configured to receive input from a computer user;

the at least one electronic data processor configured to execute a first web browser process, capable of accessing data of the at least one website via the network, in a first logical process within the common operating system, wherein the first logical process is capable of accessing data contained in the first memory space;

the at least one electronic data processor further configured to execute a second web browser process in a second logical process within the common operating system, wherein the second logical process is capable of accessing data contained in the second memory space and is further capable of generating video data from the at least one website accessed via the network;

and

a video processor configured to process video data from the second web browser process for display;

wherein the first web browser process is capable of opening the second web browser process and is further capable of passing data to the second web browser process;

wherein further the portable computer is configured such that the at least one system file



residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing within the second web browser process.

22. (New) The portable computer of Claim 21 wherein the first web browser process is capable of directly exchanging data with the network interface device and with the second web browser process.

23. (New) The portable computer of Claim 22 wherein the first web browser process is capable of passing data downloaded from the network to the second web browser process.

24. (New) The portable computer of Claim 21 wherein the second web browser process is capable of directly exchanging data with the network interface device and with the first web browser process.

25. (New) The portable computer of Claim 21 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

\_\_\_\_\_ an Application Specific Integrated Circuit;

\_\_\_\_\_ a Field Programmable Gate Array;

\_\_\_\_\_ a plurality of electronic data processors; and

\_\_\_\_\_ a multi-core electronic data processor.

26. (New) The portable computer of Claim 21 wherein the second memory space comprises memory selected from the group consisting of:

\_\_\_\_\_ a memory zone within a physical memory common to the first memory space;

\_\_\_\_\_ a partition on a memory device;

\_\_\_\_\_ random access memory (RAM); and

\_\_\_\_\_ both volatile and nonvolatile memory.

27. (New) The portable computer of Claim 21 configured such that at least one corrupted file required for a web browser process is capable of being restored from a protected image.

28. (New) The portable computer of Claim 27 wherein the protected image is stored at a location selected from the group consisting of:

\_\_\_\_\_ a removable drive;

\_\_\_\_\_ the first memory space;

\_\_\_\_\_ a partition on a memory device; and

\_\_\_\_\_ a nonvolatile memory disk.

29. (New) The portable computer of Claim 21 configured to close the second web browser process and automatically delete at least one file selected from the group consisting of a temporary internet file, a cookie and a corrupted file.

30. (New) The portable computer of Claim 21 configured such that the first web browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second web browser process.

31. (New) The portable computer of Claim 21 wherein attempts by malware to record data entry by the computer user are effectively blocked.

32. (New) A method of operating a portable computer capable of executing instructions using a common operating system and having at least one electronic data processor communicatively coupled to a first and second memory space and to a network interface device, comprising:

\_\_\_\_\_ exchanging data across a network of one or more computers with the network interface device and accessing at least one website;

storing at least one system file within the first memory space;  
executing a first web browser process, capable of accessing data of the at least one website via the network, in a first logical process within the common operating system using the at least one electronic data processor, wherein the first logical process is configured to access data contained in the first memory space;  
executing a second web browser process in a second logical process within the common operating system using the at least one electronic data processor, wherein the second logical process is configured to access data contained in the second memory space and is further configured to generate video data;  
opening the second web browser process on instruction from the first web browser process;  
passing data from the first web browser process to the second web browser process; and  
displaying website video data from the second web browser process;  
wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser process.

33. (New) The method of Claim 32 wherein the portable computer is configured such that the first web browser process is capable of directly exchanging data with the network interface device and with the second web browser process.

34. (New) The method of Claim 33 and further comprising downloading data from the network and passing the data from the first web browser process to the second web browser process.

35. (New) The method of Claim 32 wherein the portable computer is configured such that the second web browser process is capable of directly exchanging data with the network interface device and with the first web browser process.

36. (New) The method of Claim 32 wherein the second memory space comprises memory selected from the group consisting of:

\_\_\_\_\_ a memory zone within a physical memory common to the first memory space;

\_\_\_\_\_ a partition on a memory device;

\_\_\_\_\_ random access memory (RAM); and

\_\_\_\_\_ both volatile and nonvolatile memory.

37. (New) The method of Claim 32 and further comprising —restoring at least one corrupted file from a protected image.

38. (New) The method of Claim 37 wherein the protected image is stored at a location selected from the group consisting of:

\_\_\_\_\_ a removable drive;

\_\_\_\_\_ the first memory space;

\_\_\_\_\_ a partition on a memory device; and

\_\_\_\_\_ a nonvolatile memory disk.

39. (New) The method of Claim 32 and further comprising —deleting at least one corrupted data file residing on the second memory space when the second logical process is terminated.

40. (New) The method of Claim 32 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

\_\_\_\_\_ an Application Specific Integrated Circuit;

a Field Programmable Gate Array;

a plurality of electronic data processors; and

a multi-core electronic data processor.

41. (New) The method of Claim 32 wherein the first web browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second web browser process.

42. (New) The method of Claim 32 and further comprising displaying video data from the first web browser process.

43. (New) The method of Claim 32 wherein attempts by malware to record data entry by the computer user are effectively blocked.

44. (New) A method of operating a portable computer capable of executing instructions using a common operating system and comprising a network interface device, at least a first memory space and a second memory space, and at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, comprising:

exchanging data across a network of one or more computers with the network interface device and accessing at least one website;

storing at least one system file in the first memory space;

opening a first web browser process capable of accessing data of the at least one website via the network, wherein the first web browser process is capable of accessing data contained in the first memory space;

opening a second web browser process, wherein the second web browser process is capable of accessing data contained in the second memory space, and is further capable of

generating data for video display; and

\_\_\_\_\_ passing data from the first web browser process to the second web browser process;

\_\_\_\_\_ wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser process.

45. (New) The method of Claim 44 wherein the first web browser process is capable of directly exchanging data with the network interface device and with the second web browser process.

46. (New) The method of Claim 45 and further comprising —downloading data from the network and passing the downloaded data from the first web browser process to the second web browser process.

47. (New) The method of Claim 46 and further comprising storing the downloaded data on the second memory space.

48. (New) The method of Claim 44 wherein the second web browser process is capable of directly exchanging data with the network interface device and with the first web browser process.

49. (New) The method of Claim 44 and further comprising —restoring at least one corrupted file from a protected image.

50. (New) The method of Claim 49 wherein the protected image is stored at a location selected from the group consisting of:

\_\_\_\_\_ a removable drive;

\_\_\_\_\_ the first memory space;

\_\_\_\_\_ a partition on a memory device; and  
\_\_\_\_\_ a non-volatile memory disk.

51. (New) The method of Claim 44 further comprising closing the second web browser process and automatically deleting at least one file selected from the group consisting of a temporary internet file, a cookie and a corrupted file.

52. (New) The method of Claim 44 wherein the first web browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second web browser process.

53. (New) The method of Claim 44 and further comprising the first web browser process instructing the second web browser process to open.

54. (New) The method of Claim 44 wherein attempts by malware to record data entry by a computer user are effectively blocked.

55. (New) The method of Claim 44 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

\_\_\_\_\_ an Application Specific Integrated Circuit;

\_\_\_\_\_ a Field Programmable Gate Array;

\_\_\_\_\_ a plurality of electronic data processors; and

\_\_\_\_\_ a multi-core electronic data processor.

56. (New) The method of Claim 44 wherein the second memory space comprises memory selected from the group consisting of:

\_\_\_\_\_ a memory zone within a physical memory common to the first memory space;

\_\_\_\_\_ a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

57. (New) The method of Claim 44 and further comprising the first web browser process opening a plurality of second web browser processes.

58. (New) The portable computer of Claim 21 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

59. (New) The portable computer of Claim 58 wherein the network comprises a cellular data carrier network.

60. (New) The method of Claim 32 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

61. (New) The method of Claim 60 wherein the network comprises a cellular data carrier network.

62. (New) The method of Claim 44 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

63. (New) The method of Claim 62 wherein the network comprises a cellular data carrier network.

64. (New) A computer program product comprising a program code stored in a non-transitory computer readable medium operable on computer capable of executing instructions using a common operating system and having at least one electronic data processor communicatively coupled to a first and second memory space and to a network interface device configured to exchange data across a network of one or more computers and access at least one website, configured to:

store at least one system file within the first memory space;



\_\_\_\_\_ open a first web browser process, capable of accessing data of the at least one website via the network, in a first logical process, the first logical process being configured to access data contained in the first memory space;

\_\_\_\_\_ open a second web browser process in a second logical process, the second logical process being configured to access data contained in the second memory space; and

\_\_\_\_\_ pass data from the first web browser process to the second web browser process, wherein the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser process.

65. \_\_\_\_\_ (New) The computer program product of Claim 64 wherein the first web browser process is capable of opening the second web browser process and the program code stored in the non-transitory computer readable medium is further configured to pass data to the second web browser process.

66. \_\_\_\_\_ (New) The computer program product of Claim 64 wherein the second logical process is configured to generate data for display and the program code stored in the non-transitory computer readable medium is further configured to process website video data from the second web browser process.

67. \_\_\_\_\_ (New) The computer program product of Claim 64 wherein the first web browser process is capable of directly exchanging data with the network interface device and the second web browser process or the second web browser process is capable of directly exchanging data with the network interface device and the first web browser process.

68. \_\_\_\_\_ (New) The computer program product of Claim 64 wherein at least one corrupted file for a web browser process is capable of being restored from a protected file.

69. (New) The computer program product of Claim 64 configured to close the second web browser process and automatically delete at least one file selected from the group consisting of a temporary internet file, a cookie and a corrupted file.

70. (New) The computer program product of Claim 64 wherein the first web browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second web browser process.

71. (New) The computer program product of Claim 64 wherein attempts by malware to record data entry by a computer user are effectively blocked.

72. (New) The computer program product of Claim 64 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

73. (New) The computer program product of Claim 72 wherein the network comprises a cellular data carrier network.

## REMARKS

The Applicants have carefully considered this application in connection with the Examiner's Office Action and respectfully request reconsideration of this application in view of the foregoing amendments and the following remarks.

The Applicants previously submitted Claims 1-73 in the application. While Claims 1, 10, 15, 21-24, 27, 29, 30, 32-35, 41, 42, 44-46, 48, 51-53, 57 and 64-70 have been amended, no claims have been cancelled herein. For the Examiner's benefit, the Applicants have provided an Appendix II to clearly show the amendments to the specification and claims from the amendment filed on April 29, 2011. Also, the Examiner has indicated that Claims 8, 9, 13 and 18 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Accordingly, Claims 1-73 are currently pending in the application.

### **I. Rejections under 35 U.S.C. §102**

The Examiner has rejected Claims 1, 2, 4, 5, 7, 10-12, 14-17, 19, 21-26, 29-48, 51-56, 58-67 and 69-73 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent Application Publication No. 2002/0002673 to Narin. As the Examiner is no doubt aware, anticipation requires that each and every limitation of the claimed invention be disclosed in a single prior art reference. The disclosed limitations must either be disclosed expressly or inherently and must be arranged as in the rejected claims.

Regarding independent Claims 1, 10, 15, 21, 32, 44 and 64 of the present application, the Applicants have amended the claims in accordance with the Examiner suggestion to further the prosecution thereof in an expeditious manner. (Examiner's Office Action, pp. 2-4.) In

accordance therewith, the Applicants believe that Narin does not disclose a computer system, portable computer, computer program product or related method as recited in ones of independent Claims 1, 10, 15, 21, 32, 44 and 64 of the present application. In particular, the Applicants believe that Narin fails to disclose, among other things, a computer system, portable computer, computer program product or related method configured to execute (or open) a first web browser process capable of accessing data of a website via a network of one or more computers (*e.g.*, the internet) as recited in ones of independent Claims 1, 10, 15, 21, 32, 44 and 64 of the present application.

Narin, therefore, fails to disclose the limitations of independent Claims 1, 10, 15, 21, 32, 44 and 64, and the claims dependent thereon. Accordingly, the Applicants respectfully request the Examiner to withdraw the §102 rejection in view thereof with respect to Claims 1, 2, 4, 5, 7, 10-12, 14-17, 19, 21-26, 29-48, 51-56, 58-67 and 69-73 of the present application.

## **II. Rejections under 35 U.S.C. §103(a)**

The Examiner has rejected Claims 3 and 57 under 35 U.S.C. § 103(a) as being unpatentable over Narin. The Examiner has rejected Claims 6, 20, 27, 28, 37, 38, 49, 50 and 68 under 35 U.S.C. § 103(a) as being unpatentable over Narin in view of U.S. Patent No. 7,024,581 to Wang, *et al.* (“Wang”). For the reasons as set forth herein, Narin fails to teach or suggest a method of operating a computer system, a multi-processor computer system, a portable computer and method of operating the same, and a computer program product as recited in ones of independent Claims 1, 15, 21, 32, 44 and 64, and Wang fails to cure the deficiencies thereof. Thus, since Narin fails to teach or suggest all of the limitations of independent Claims 1, 15, 21, 32, 44 and 64, and the secondary reference fails to cure the deficiencies thereof, the Examiner

cannot establish a *prima facie* case of obviousness of Claims 3, 6, 20, 27, 28, 37, 38, 49, 50, 57 and 68, which depend from ones thereof. Accordingly, the Applicants respectfully request the Examiner to withdraw the §103 rejection with respect to Claims 3, 6, 20, 27, 28, 37, 38, 49, 50, 57 and 68 of the present application.

### **III. Double Patenting**

The Examiner has provisionally rejected Claims 21-73 on the grounds of nonstatutory double patenting over Claims 21-55 of co-pending U.S. Patent Application Serial No. 12/720,207 to Rozman, *et al.* Although the Applicants do not necessarily agree, the Applicant has filed a Terminal Disclaimer herewith directed to U.S. Patent Application Serial No. 12/720,207 in compliance with 37 CFR §1.321 to overcome the Examiner's rejection thereto.

#### IV. Conclusion

In view of the foregoing amendments and remarks, the Applicants now see all of the claims currently pending in this application to be in condition for allowance and therefore earnestly solicit a Notice of Allowance therefor.

The Applicants request that the Examiner telephone the undersigned attorney of record at (972) 732-1001 if such would further expedite the prosecution of the present application. If the enclosed fees are insufficient, the Commissioner is hereby authorized to charge any additional fees, or credit any overpayments, to Deposit Account No. 50-1065.

Respectfully submitted,

January 24, 2012

Date

/Glenn W. Boisbrun/

Glenn W. Boisbrun  
Attorney for Applicant  
Reg. No. 39,615

Slater & Matsil, L.L.P.  
17950 Preston Rd., Suite 1000  
Dallas, Texas 75252-5793  
Tel. 972-732-1001  
Fax: 972-732-9218

**APPENDIX I**

**STATUS OF CLAIMS AND  
SUPPORT FOR CLAIM CHANGES**

<b>Claims</b>	<b>Status</b>	<b>Support</b>		
1	Four Times Amended	Col 9 lines 30-37 Fig. 1, 190, 195 Col 18 lines 3-5	Col 11 lines 2-4 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Claim 3
2	Twice Amended	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
3	Twice Amended	Col 18 lines 6-10		
4	Original			
5	Original			
6	Twice Amended	Fig. 4, 420	Col 12 lines 46-58	
7	Amended	Col 18 lines 49-52		
8	Amended	Col 18 lines 53-60		
9	Amended	Col 18 lines 61-65		
10	Four Times Amended	Col 9 lines 30-37 Fig. 1, 190, 195 Col 18 lines 3-5	Col 11 lines 2-4 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Claim 3
11	Twice Amended	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
12	Original			
13	Original			
14	Original			
15	Four Times Amended	Col 9 lines 30-37 Fig. 1, 190, 195	Col 11 lines 2-4 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Claim 3
16	Original			
17	Twice Amended	Fig. 1, 120, 191, 190, 110, 130		
18	Original			
19	Amended	Col 20 lines 38-42		
20	Twice Amended	Fig. 4, 420	Col 12 lines 46-58	
21	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53	Fig. 1, 120, 150, 160 Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 23-28 Col 18 lines 3-5

		Fig. 1, 120, 191, 190, 110, 130	Col 11 lines 2-4 Col 8 lines 1-6	Claim 3
22	New	Fig. 1, 120, 191, 190		
23	New	Fig. 1, 120, 191, 190, 195	Col 11 lines 38-41	
24	New	Fig. 1, 140, 190		
25	New	Col 14 lines 62-67	Col 9 lines 30-47	
26	New	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
27	New	Fig. 4, 420	Col 12 lines 46-58	
28	New	Col 12 lines 46-58	Col 7 lines 13-16	
29	New	Col 8 lines 23-26		
30	New	Col 19 lines 33-37		
31	New	Col 7 lines 58-62		
32	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Col 11 lines 2-4 Col 8 lines 1-6	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 23-28 Claim 3
33	New	Fig. 1, 120, 191, 190		
34	New	Fig. 1, 120, 191, 190, 195	Col 11 lines 38-41	
35	New	Fig. 1, 140, 190		
36	New	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
37	New	Fig. 4, 420	Col 12 lines 46-58	
38	New	Col 12 lines 46-58	Col 7 lines 13-16	
39	New	Col 8 lines 23-26		
40	New	Col 14 lines 62-67	Col 9 lines 30-47	
41	New	Col 19 lines 33-37		
42	New	Fig. 1, 120, 170, 171, 180		
43	New	Col 7 lines 58-62		
44	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Col 11 lines 2-4 Col 8 lines 1-6	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 25-28 Claim 3
45	New	Fig. 1, 120, 191, 190		
46	New	Fig. 1, 120, 191, 190, 195	Col 11 lines 38-41	
47	New	Fig. 3, 320		
48	New	Fig. 1, 140, 190		



49	New	Fig. 4, 420	Col 12 lines 46-58	
50	New	Col 12 lines 46-58	Col 7 lines 13-16	
51	New	Col 8 lines 23-26		
52	New	Col 19 lines 33-37		
53	New	Fig 2. 220		
54	New	Col 7 lines 58-62		
55	New	Col 14 lines 62-67	Col 9 lines 30-47	
56	New	Col 18 lines 30-33	Col 16 lines 19-21 Col 16 lines 44-47	Col 9 lines 48-52 Col 10 lines 34-37
57	New	Col 13 lines 22-24	Fig 2, 220	
58	New	Col 10 lines 19-22		
59	New	Col 1 and 2	US PAT 6,216,112	
60	New	Col 10 lines 19-22		
61	New	Col 1 and 2	US PAT 6,216,112	
62	New	Col 10 lines 19-22		
63	New	Col 1 and 2	US PAT 6,216,112	
64	New	Col 9 lines 30-37 Fig. 1, 190 Col 7 lines 63-67 Col 9 line 53 Fig. 1, 120, 191, 190, 110, 130	Col 16 lines 24-30 Col 6 lines 56-60 Col 10 line 67 Col 11 lines 2-4 Col 8 lines 1-6	Fig. 1, 120, 140 Fig. 1, 140, 170, 180 Col 18 lines 25-28 Claim 3
65	New	Fig. 1, 120, 191, 190, 195	Col 11 lines 38-41 Col 13 lines 22-24	Fig 2, 220
66	New	Fig. 1		
67	New	Fig. 1, 120, 191, 190		
68	New	Fig. 4, 420	Col 12 lines 46-58	
69	New	Col 8 lines 23-26		
70	New	Col 19 lines 33-37		
71	New	Col 7 lines 58-62		
72	New	Col 10 lines 19-22		
73	New	Col 1 and 2	US PAT 6,216,112	

## APPENDIX II

### SPECIFICATION AS AMENDED ACCORDING TO STANDARD AMENDMENT FORMAT

Kindly amend the “Cross Reference to Multiple Reissue Applications” section as set forth below:

#### Cross Reference to Multiple Reissue Applications

This application is a reissue application of U.S. Patent No. 7,484,247, entitled “System and Method for Protecting a Computer System from Malicious Software,” issued on January 27, 2009, and is related to another reissue application designated U.S. Patent Application Serial No. 12/720,207 from U.S. Patent No. 7,484,247 filed concurrently herewith, which are incorporated herein by reference. This application is also related to another reissue application designated U.S. Patent Application Serial No. 12/854,149 (now, U.S. Patent No. RE43,103) from U.S. Patent No. 7,484,247 filed on August 10, 2010 and a continuation application therefrom designated U.S. Patent Application Serial No. 13/015,186 filed on January 27, 2011, which are incorporated herein by reference. This application is also related to another reissue application designated U.S. Patent Application Serial No. 12/941,067 from U.S. Patent No. 7,484,247 filed on November 7, 2010, which is incorporated herein by reference.

## CLAIMS AS AMENDED ACCORDING TO STANDARD AMENDMENT FORMAT

1. (Currently Amended) A method of operating a computer system capable of exchanging data across a network of one or more computers and having at least a first and second electronic data processor capable of executing instructions using a common operating system, comprising:

executing a first web browser process, capable of accessing data of a website via the network, in a first logical process within the common operating system using the first electronic data processor, wherein the first logical process is capable of accessing data contained in a first memory space;

executing a second web browser process in a second logical process within the common operating system using the second electronic data processor, wherein the second logical process is capable of accessing data contained in the second memory space; and

displaying data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to a display;

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser process.

2. (Previously Presented) The method of claim 1 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

3. (Previously Presented) The method of claim 1 wherein the first logical process is capable of accessing data contained in the second memory spaces.

4. (Previously Presented) The method of claim 1 wherein the first logical process receives user interface data, and passes the user interface data to the second logical process.

5. (Previously Presented) The method of claim 1 wherein the first and second electronic data processors are part of a multi-core electronic data processor.

6. (Previously Presented) The method of claim 1 and further comprising restoring at least one corrupted data file from a protected image.

7. (Previously Presented) The method of claim 1 and further comprising automatically deleting at least one data file residing on the second memory space when the second logical process is terminated.

8. (Previously Presented) The method of claim 1 and further comprising:  
encrypting data with the first logical process;  
transferring the encrypted data from the first logical process to the second logical process; and

transferring the encrypted data from the second logical process to the network interface device.

9. (Previously Presented) The method of claim 8 and further comprising:

decrypting the data with the network interface device; and

transferring the decrypted data from the network interface device to the network.

10. (Currently Amended) A multi-processor computer system using a common operating system capable of exchanging data across a network of one or more computers via a network interface device, comprising:

a first electronic data processor capable of executing a first web browser process using the common operating system and communicatively coupled to a first memory space, the first web browser process capable of accessing data of a website via the network;

a second electronic data processor capable of executing a second web browser process using the common operating system and communicatively coupled to a second memory space; and

a video processor adapted to combine video data from the first and second electronic data processors and transmit the combined video data to a display;

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser process.

11. (Previously Presented) The computer system of claim 10 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and  
both volatile and nonvolatile memory.

12. (Previously Presented) The computer system of claim 10 wherein the first and second electronic data processors are part of a dual processor computer system.

13. (Previously Presented) The computer system of claim 10 wherein the second electronic data processor and the video processor are co-located on a circuit card, the circuit card being communicatively coupled to the first electronic data processor.

14. (Previously Presented) The computer system of claim 10 wherein the computer system is configured such that the first electronic data processor is protected from executing instructions initiated by a malware process downloaded from the network and executing on the second electronic data processor.

15. (Currently Amended) A multi-processor computer system using a common operating system capable of exchanging data across a network of one or more computers, comprising:

at least a first and second electronic data processor capable of executing instructions using the common operating system;

at least a first and second memory space; and

a video processor;

wherein the first and second electronic data processors, first and second memory space, and video processor are configured to:

execute a first web browser process, capable of accessing data of a website via the network, in a first logical process with the first electronic data processor, wherein the first logical process is executing within the common operating system and is capable of accessing data

contained in the first memory space;

execute a second web browser process in a second logical process with the second electronic data processor, wherein the second logical process is executing within the common operating system and is capable of accessing data contained in the second memory space; and

display data from the first logical process and the second logical process, wherein the video processor is adapted to combine data from the first and second logical processes and transmit the combined data to a display;

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser process.

16. (Previously Presented) The computer system of claim 15 wherein the computer system is further configured such that the first logical process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second logical process.

17. (Previously Presented) The computer system of claim 15 and further comprising at least one network interface device capable of exchanging data with the network and with a logical process that comprises a process selected from the group consisting of:

the first logical process; and

the second logical process.

18. (Previously Presented) The computer system of claim 17 wherein the network interface device is capable of decrypting data received from the second logical process and

transmitting the decrypted data to the network while preventing the second logical process from accessing the decrypted data.

19. (Previously Presented) The computer system of claim 15 wherein the at least one electronic data processor comprises a processor selected from the group consisting of a multi-core electronic data processor; dual electronic data processors; and multiple electronic data processors.

20. (Previously Presented) The computer system of claim 15 and further configured to restore-at least one corrupted data file from a protected image.

21. (Currently Amended) A portable computer capable of executing instructions using a common operating system, comprising:

a network interface device configured to exchange data across a network of one or more computers and access at least one website;

at least a first memory space and a second memory space, the first memory space containing at least one system file;

at least one electronic data processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, wherein the user interface is configured to receive input from a computer user;

the at least one electronic data processor configured to execute a first web browser process, capable of accessing data of the at least one website via the network, in a first logical process within the common operating system, wherein the first logical process is capable of accessing data contained in the first memory space;

the at least one electronic data processor further configured to execute a second web browser process in a second logical process within the common operating system, wherein the



second logical process is capable of accessing data contained in the second memory space and is further capable of generating video data from [[a]]the at least one website accessed via the network; and

a video processor configured to process video data from the second web browser process for display;

wherein the first web browser process is capable of opening the second web browser process and is further capable of passing data to the second web browser process;

wherein further the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing within the second web browser process.

22. (Currently Amended) The portable computer of Claim 21 wherein the first web browser process is capable of directly exchanging data with the network interface device and with the second web browser process.

23. (Currently Amended) The portable computer of Claim 22 wherein the first web browser process is capable of passing data downloaded from the network to the second web browser process.

24. (Currently Amended) The portable computer of Claim 21 wherein the second web browser process is capable of directly exchanging data with the network interface device and with the first web browser process.

25. (Previously Presented) The portable computer of Claim 21 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

an Application Specific Integrated Circuit;

a Field Programmable Gate Array;

a plurality of electronic data processors; and  
a multi-core electronic data processor.

26. (Previously Presented) The portable computer of Claim 21 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;  
a partition on a memory device;  
random access memory (RAM); and  
both volatile and nonvolatile memory.

27. (Currently Amended) The portable computer of Claim 21 configured such that at least one corrupted file required for a web browser process is capable of being restored from a protected image.

28. (Previously Presented) The portable computer of Claim 27 wherein the protected image is stored at a location selected from the group consisting of:

a removable drive;  
the first memory space;  
a partition on a memory device; and  
a nonvolatile memory disk.

29. (Currently Amended) The portable computer of Claim 21 configured ~~such that at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated~~ to close the second web browser process and automatically delete at least one file selected from the group consisting of a temporary internet file, a cookie and a corrupted file.

30. (Currently Amended) The portable computer of Claim 21 configured such that the first web browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second web browser process.

31. (Previously Presented) The portable computer of Claim 21 wherein attempts by malware to record data entry by the computer user are effectively blocked.

32. (Currently Amended) A method of operating a portable computer capable of executing instructions using a common operating system and having at least one electronic data processor communicatively coupled to a first and second memory space and to a network interface device, comprising:

exchanging data across a network of one or more computers with the network interface device and accessing at least one website;

storing at least one system file within the first memory space;

executing a first web browser process, capable of accessing data of the at least one website via the network, in a first logical process within the common operating system using the at least one electronic data processor, wherein the first logical process is configured to access data contained in the first memory space;

executing a second web browser process in a second logical process within the common operating system using the at least one electronic data processor, wherein the second logical process is configured to access data contained in the second memory space and is further configured to generate video data;

opening the second web browser process on instruction from the first web browser process;

passing data from the first web browser process to the second web browser process; and

displaying website video data from the second web browser process;

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser process.

33. (Currently Amended) The method of Claim 32 wherein the portable computer is configured such that the first web browser process is capable of directly exchanging data with the network interface device and with the second web browser process.

34. (Currently Amended) The method of Claim 33 and further comprising downloading data from the network and passing the data from the first web browser process to the second web browser process.

35. (Currently Amended) The method of Claim 32 wherein the portable computer is configured such that the second web browser process is capable of directly exchanging data with the network interface device and with the first web browser process.

36. (Previously Presented) The method of Claim 32 wherein the second memory space comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

37. (Previously Presented) The method of Claim 32 and further comprising restoring at least one corrupted file from a protected image.

38. (Previously Presented) The method of Claim 37 wherein the protected image is stored at a location selected from the group consisting of:

a removable drive;  
the first memory space;  
a partition on a memory device; and  
a nonvolatile memory disk.

39. (Previously Presented) The method of Claim 32 and further comprising deleting at least one corrupted data file residing on the second memory space when the second logical process is terminated.

40. (Previously Presented) The method of Claim 32 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

an Application Specific Integrated Circuit;  
a Field Programmable Gate Array;  
a plurality of electronic data processors; and  
a multi-core electronic data processor.

41. (Currently Amended) The method of Claim 32 wherein the first web browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second web browser process.

42. (Currently Amended) The method of Claim 32 and further comprising displaying video data from the first web browser process.

43. (Previously Presented) The method of Claim 32 wherein attempts by malware to record data entry by the computer user are effectively blocked.

44. (Currently Amended) A method of operating a portable computer capable of executing instructions using a common operating system and comprising a network interface device, at least a first memory space and a second memory space, and at least one electronic data

processor communicatively coupled to the network interface device, the first and second memory space, and to a user interface, comprising:

exchanging data across a network of one or more computers with the network interface device and accessing at least one website;

storing at least one system file in the first memory space;

opening a first web browser process capable of accessing data of the at least one website via the network, wherein the first web browser process is capable of accessing data contained in the first memory space;

opening a second web browser process, wherein the second web browser process is capable of accessing data contained in the second memory space, and is further capable of generating data for video display; and

passing data from the first web browser process to the second web browser process;

wherein the portable computer is configured such that the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser process.

45. (Currently Amended) The method of Claim 44 wherein the first web browser process is capable of directly exchanging data with the network interface device and with the second web browser process.

46. (Currently Amended) The method of Claim 45 and further comprising downloading data from the network and passing the downloaded data from the first web browser process to the second web browser process.

47. (Previously Presented) The method of Claim 46 and further comprising storing the downloaded data on the second memory space.

48. (Currently Amended) The method of Claim 44 wherein the second web browser process is capable of directly exchanging data with the network interface device and with the first web browser process.

49. (Previously Presented) The method of Claim 44 and further comprising restoring at least one corrupted file from a protected image.

50. (Previously Presented) The method of Claim 49 wherein the protected image is stored at a location selected from the group consisting of:

a removable drive;

the first memory space;

a partition on a memory device; and

a non-volatile memory disk.

51. (Currently Amended) The method of Claim 44 ~~wherein at least one corrupted file residing on the second memory space is capable of being automatically deleted when the second browser process is terminated~~ further comprising closing the second web browser process and automatically deleting at least one file selected from the group consisting of a temporary internet file, a cookie and a corrupted file.

52. (Currently Amended) The method of Claim 44 wherein the first web browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second web browser process.

53. (Currently Amended) The method of Claim 44 and further comprising the first web browser process instructing the second web browser process to open.

54. (Previously Presented) The method of Claim 44 wherein attempts by malware to record data entry by a computer user are effectively blocked.

55. (Previously Presented) The method of Claim 44 wherein the at least one electronic data processor comprises a processor selected from the group consisting of:

- an Application Specific Integrated Circuit;
- a Field Programmable Gate Array;
- a plurality of electronic data processors; and
- a multi-core electronic data processor.

56. (Previously Presented) The method of Claim 44 wherein the second memory space comprises memory selected from the group consisting of:

- a memory zone within a physical memory common to the first memory space;
- a partition on a memory device;
- random access memory (RAM); and
- both volatile and nonvolatile memory.

57. (Currently Amended) The method of Claim 44 and further comprising the first web browser process opening a plurality of second web browser processes.

58. (Previously Presented) The portable computer of Claim 21 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

59. (Previously Presented) The portable computer of Claim 58 wherein the network comprises a cellular data carrier network.

60. (Previously Presented) The method of Claim 32 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

61. (Previously Presented) The method of Claim 60 wherein the network comprises a cellular data carrier network.



62. (Previously Presented) The method of Claim 44 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

63. (Previously Presented) The method of Claim 62 wherein the network comprises a cellular data carrier network.

64. (Currently Amended) A computer program product comprising a program code stored in a non-transitory computer readable medium operable on computer capable of executing instructions using a common operating system and having at least one electronic data processor communicatively coupled to a first and second memory space and to a network interface device configured to exchange data across a network of one or more computers and access at least one website, configured to:

store at least one system file within the first memory space;

open a first web browser process, capable of accessing data of the at least one website via the network, in a first logical process, the first logical process being configured to access data contained in the first memory space;

open a second web browser process in a second logical process, the second logical process being configured to access data contained in the second memory space; and

pass data from the first web browser process to the second web browser process, wherein the at least one system file residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser process.

65. (Currently Amended) The computer program product of Claim 64 wherein the first web browser process is capable of opening the second web browser process and the program

code stored in the non-transitory computer readable medium is further configured to pass data to the second web browser process.

66. (Currently Amended) The computer program product of Claim 64 wherein the second logical process is configured to generate data for display and the program code stored in the non-transitory computer readable medium is further configured to process website video data from the second web browser process.

67. (Currently Amended) The computer program product of Claim 64 wherein the first web browser process is capable of directly exchanging data with the network interface device and the second web browser process or the second web browser process is capable of directly exchanging data with the network interface device and the first web browser process.

68. (Currently Amended) The computer program product of Claim 64 wherein at least one corrupted file for a web browser process is capable of being restored from a protected file.

69. (Currently Amended) The computer program product of Claim 64 ~~wherein at least one corrupted file residing on the second memory space is capable of being deleted when the second browser process is terminated~~ configured to close the second web browser process and automatically delete at least one file selected from the group consisting of a temporary internet file, a cookie and a corrupted file.

70. (Currently Amended) The computer program product of Claim 64 wherein the first web browser process is protected from executing instructions initiated by a malware process downloaded from the network and executing as part of the second web browser process.

71. (Previously Presented) The computer program product of Claim 64 wherein attempts by malware to record data entry by a computer user are effectively blocked.

72. (Previously Presented) The computer program product of Claim 64 wherein the network interface device is capable of exchanging data with the network using a wireless connection.

73. (Previously Presented) The computer program product of Claim 72 wherein the network comprises a cellular data carrier network.



Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>Request for Continued Examination (RCE) Transmittal</b>  Address to: Mail Stop RCE Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450	Application Number	12/720,147
	Filing Date	March 9, 2010
	First Named Inventor	Rozman, <i>et al.</i>
	Art Unit	2439
	Examiner Name	Christian A. LaForgia
	Attorney Docket Number	ARAC-01RE1

**This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.**

Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1.  Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).
- a.  Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.
- i.  Consider the arguments in the Appeal Brief or Reply Brief previously filed on \_\_\_\_\_
- ii.  Other \_\_\_\_\_
- b.  Enclosed
- i.  Amendment/Reply
- ii.  Affidavit(s)/Declaration(s)
- iii.  Information Disclosure Statement (IDS)
- iv.  Other \_\_\_\_\_
2.  Miscellaneous
- a.  Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of \_\_\_\_\_ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)
- b.  Other \_\_\_\_\_
3.  Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
- a.  The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments, to Deposit Account No. 50-1065.
- i.  RCE fee required under 37 CFR 1.17(e)
- ii.  Extension of time fee (37 CFR 1.136 and 1.17)
- iii.  Other Terminal Disclaimer Fee
- b.  Check in the amount of \$ \_\_\_\_\_ enclosed
- c.  Payment by credit card (Form PTO-2038 enclosed)

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.****SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED**

Signature	/Glenn W. Boisbrun/	Date	January 24, 2012
Name (Print/Type)	Glenn W. Boisbrun	Registration No.	39,615

**CERTIFICATE OF MAILING OR TRANSMISSION**

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner For Patents, P.O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature		Date	
Name (Print/Type)			

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number <b>12/720,147</b>	Filing Date <b>03/09/2010</b>	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (j), or (m))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A		N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(j))</small>	minus 20 =	*	X \$ =	OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =		X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>						
			TOTAL		TOTAL	

\* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT	<b>01/24/2012</b>	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	* 73	Minus ** 73	= 0	X \$30 =	0	OR	X \$ =
	Independent (37 CFR 1.16(h))	* 7	Minus *** 7	= 0	X \$125 =	0	OR	X \$ =
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR	
					TOTAL ADD'L FEE	<b>0</b>	OR	TOTAL ADD'L FEE

	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	X \$ =		OR	X \$ =
	Independent (37 CFR 1.16(h))	*	Minus ***	=	X \$ =		OR	X \$ =
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						OR	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE


\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:  
 /DEBORAH NASH/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

<b>Application Number</b> 	<b>Application/Control No.</b> 12/720,147	<b>Applicant(s)/Patent under Reexamination</b> ROZMAN ET AL.	

<b>Document Code - DISQ</b>	<b>Internal Document – DO NOT MAIL</b>
-----------------------------	--

<b>TERMINAL DISCLAIMER</b>	<input checked="" type="checkbox"/> <b>APPROVED</b>	<input type="checkbox"/> <b>DISAPPROVED</b>
Date Filed : 01/24/12	<b>This patent is subject to a Terminal Disclaimer</b>	

<b>Approved/Disapproved by:</b>
---------------------------------

Angie Walker
--------------





## SUPPLEMENTAL REISSUE APPLICATION DECLARATION BY THE INVENTOR

Docket Number (Optional)

ARAC-01RE1

I hereby declare that:

Each inventor's residence, mailing address and citizenship are stated below next to their name.

I believe the inventors named below to be the original and first inventor(s) of the subject matter which is described and claimed in patent number 2,492,247 granted January 27, 2009 and for which a reissue patent is sought on the invention entitled \_\_\_\_\_

System and Method for Protecting a Computer System from Malicious Software

the specification of which

is attached hereto.

was filed on March 09, 2010 as reissue application number 12/720,147

and was amended on 4/4/11, 8/29/11 and 1/24/12  
(If applicable)

I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b). Attached is form PTO/SB/02B (or equivalent) listing the foreign applications.

I verily believe the original patent to be wholly or partly inoperative or invalid, for the reasons described below. (Check all boxes that apply.)

by reason of a defective specification or drawing.

by reason of the patentee claiming more or less than he had the right to claim in the patent.

by reason of other errors.

At least one error upon which reissue is based is described below. If the reissue is a broadening reissue, such must be stated with an explanation as to the nature of the broadening:

The patentees have claimed less than they had the right to claim and have filed a broadening reissue. At least one error is limiting the display of data to a windowed format. Another error is the failure to claim subject matter disclosed in the specification including a portable computer or method wherein attempts by malware to record data entry by a computer user are effectively blocked and claims directed to a computer program product.

Every error in the patent which was corrected in the present reissue application, and is not covered by the prior declaration submitted in this application, arose without any deceptive intention on the part of the Applicants.

[Page 1 of 2]

This collection of information is required by 37 CFR 1.175. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

(REISSUE APPLICATION DECLARATION BY THE INVENTOR, page 2)		Docket Number (Optional) ARAC-01RE1	
All errors corrected in this reissue application arose without any deceptive intention on the part of the applicant.			
Note To appoint a power of attorney, use form PTO/SB/81.			
Correspondence Address: Direct all communications about the application to:			
<input checked="" type="checkbox"/> The address associated with Customer Number:		25962	
OR			
<input type="checkbox"/> Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone	Email		
<b>WARNING:</b>			
Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.			
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine and imprisonment, or both, under 18 U.S.C. 1001, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this declaration is directed.			
Full name of sole or first inventor (given name, family name) Allen F. Rozman			
Inventor's signature <i>AF Rozman</i>		Date 5-2-12	
Residence 6402 Wildlife Trail, Garland, TX 75044		Citizenship US	
Mailing Address 6402 Wildlife Trail, Garland, TX 75044			
Full name of second joint inventor (given name, family name) Alfonso J. Cioffi			
Inventor's signature <i>Alfonso J. Cioffi</i>		Date 5-2-12	
Residence 719 Mockingbird Dr., Murphy, TX 75094		Citizenship US	
Mailing Address 719 Mockingbird Dr., Murphy, TX 75094			
<input type="checkbox"/> Additional joint inventors or legal representative(s) are named on separately numbered sheets forms PTO/SB/02A or 02LR attached hereto.			

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	12703940
<b>Application Number:</b>	12720147
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	8473
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Customer Number:</b>	25962
<b>Filer:</b>	Glenn W. Boisbrun/Sherry Colgrove
<b>Filer Authorized By:</b>	Glenn W. Boisbrun
<b>Attorney Docket Number:</b>	ARAC-01RE1
<b>Receipt Date:</b>	04-MAY-2012
<b>Filing Date:</b>	09-MAR-2010
<b>Time Stamp:</b>	17:27:47
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	ARAC-01RE1_Trans_Supp_Dec. pdf	14884 <small>f76f6bfa6a2f720bfa7c08cb5354b4579476d c83</small>	no	1

### Warnings:

### Information:

2	Supp reissue dec filed in accord with MPEP 1414.01.	ARAC-01RE1_Supp_Declaratio n.pdf	920491  1f6449f061dad6ff293487e7c6114aad6ad	no	2
---	---	-------------------------------------	---	----	---

**Warnings:**

**Information:**

<b>Total Files Size (in bytes):</b>	935375
-------------------------------------	--------

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**



**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

<b>Application Number</b>  	<b>Application/Control No.</b> 12/720147	<b>Applicant(s)/Patent under Reexamination</b> REIS.REVFORM
<b>Document Code - SRNT</b>		<b>Internal Document – DO NOT MAIL</b>

<b>Original Patent Number of Patent to be reissued:</b> 7484247	<b>Notice of Reissue Published in O.G. date:</b> 4/6/2010
--	--

This reissue patent is subjected Terminal Disclaimer that

was filed during the prosecution of the reissue application  
 was of record prior to the filing of the reissue application

The maintenance fee status is:

is up to date  
 was not required

Physical surrender of the letter patent:

was made  
 was not made, but a statement of loss/inaccessibility was provided by applicant(s)  
 is not required

Final SPRE review	trs	4/20/2012
-------------------	-----	-----------



NOTICE OF ALLOWANCE AND FEE(S) DUE

25962 7590 05/14/2012
SLATER & MATSIL, L.L.P.
Ira Matsil
17950 PRESTON RD, SUITE 1000
DALLAS, TX 75252-5793

EXAMINER
LAFORGIA, CHRISTIAN A
ART UNIT PAPER NUMBER

2439

DATE MAILED: 05/14/2012

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.

12/7/20,147 03/09/2010 Allen F. Rozman ARAC-01RE1 8473

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE

Table with 7 columns: APPLN. TYPE, SMALL ENTITY, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE

nonprovisional YES \$870 \$0 \$0 \$870 08/14/2012

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

**PART B - FEE(S) TRANSMITTAL**

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 or Fax (571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

25962 7590 05/14/2012  
**SLATER & MATSIL, L.L.P.**  
 Ira Matsil  
 17950 PRESTON RD, SUITE 1000  
 DALLAS, TX 75252-5793

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

_____ (Depositor's name)
_____ (Signature)
_____ (Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/720,147	03/09/2010	Allen F. Rozman	ARAC-01RE1	8473

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	\$870	\$0	\$0	\$870	08/14/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
LAFORGIA, CHRISTIAN A	2439	726-024000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. <b>Use of a Customer Number is required.</b></p>	<p>2. For printing on the patent front page, list</p> <p>(1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 _____</p> <p>(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____</p> <p>3 _____</p>
---	---

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE \_\_\_\_\_ (B) RESIDENCE: (CITY and STATE OR COUNTRY) \_\_\_\_\_

Please check the appropriate assignee category or categories (will not be printed on the patent) :  Individual  Corporation or other private group entity  Government

<p>4a. The following fee(s) are submitted:</p> <p><input type="checkbox"/> Issue Fee</p> <p><input type="checkbox"/> Publication Fee (No small entity discount permitted)</p> <p><input type="checkbox"/> Advance Order - # of Copies _____</p>	<p>4b. Payment of Fee(s); (Please first reapply any previously paid issue fee shown above)</p> <p><input type="checkbox"/> A check is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).</p>
---	--

5. Change in Entity Status (from status indicated above)

a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.  b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature \_\_\_\_\_ Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_ Registration No. \_\_\_\_\_

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
12/720,147 03/09/2010 Allen F. Rozman ARAC-01RE1 8473

25962 7590 05/14/2012
SLATER & MATSIL, L.L.P.
Ira Matsil
17950 PRESTON RD, SUITE 1000
DALLAS, TX 75252-5793

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT PAPER NUMBER

2439

DATE MAILED: 05/14/2012

Determination of Patent Term Extension or Adjustment under 35 U.S.C. 154 (b)

A reissue patent is for "the unexpired part of the term of the original patent." See 35 U.S.C. 251. Accordingly, the above-identified reissue application is not eligible for Patent Term Extension or Adjustment under 35 U.S.C. 154(b).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.



## Privacy Act Statement

**The Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

**Notice of Allowability**

**Application No.**

12/720,147

**Examiner**

Christian LaForgia

**Applicant(s)**

ROZMAN ET AL.

**Art Unit**

2439

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

- 1.  This communication is responsive to 24 January 2012.
- 2.  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
- 3.  The allowed claim(s) is/are 1-73.
- 4.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a)  All    b)  Some\*    c)  None    of the:
    - 1.  Certified copies of the priority documents have been received.
    - 2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    - 3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has **THREE MONTHS FROM THE "MAILING DATE"** of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

- 5.  A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  - 6.  CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
    - (a)  including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
      - 1)  hereto or 2)  to Paper No./Mail Date \_\_\_\_\_.
    - (b)  including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
- 7.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- 1.  Notice of References Cited (PTO-892)
- 2.  Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3.  Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 1/24/12
- 4.  Examiner's Comment Regarding Requirement for Deposit of Biological Material
- 5.  Notice of Informal Patent Application
- 6.  Interview Summary (PTO-413), Paper No./Mail Date \_\_\_\_\_.
- 7.  Examiner's Amendment/Comment
- 8.  Examiner's Statement of Reasons for Allowance
- 9.  Other \_\_\_\_\_.

/Christian LaForgia/  
Primary Examiner, Art Unit 2439

<b>Notice of References Cited</b>	Application/Control No. 12/720,147	Applicant(s)/Patent Under Reexamination ROZMAN ET AL.	
	Examiner Christian LaForgia	Art Unit 2439	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-2004/0230794 A1	11-2004	England et al.	713/164
*	B US-2005/0091661 A1	04-2005	Kurien et al.	719/310
	C US-			
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			

**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

**NON-PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
 Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.







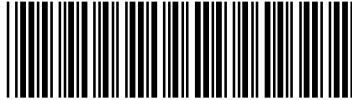
UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 8473

<b>SERIAL NUMBER</b> 12/720,147	<b>FILING or 371(c) DATE</b> 03/09/2010 <b>RULE</b>	<b>CLASS</b> 726	<b>GROUP ART UNIT</b> 2439	<b>ATTORNEY DOCKET NO.</b> ARAC-01RE1	
<b>APPLICANTS</b> Allen F. Rozman, Garland, TX; Alfonso J. Cioffi, Murphy, TX; <b>** CONTINUING DATA *****</b> This application is a REI of 10/913,609 08/07/2004 PAT 7,484,247 <b>** FOREIGN APPLICATIONS *****</b> <b>** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY **</b> 03/11/2010					
Foreign Priority claimed <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No 35 USC 119(a-d) conditions met <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Verified and /CHRISTIAN A LAFORGIA/ Acknowledged Examiner's Signature	<input type="checkbox"/> Met after Allowance Initials	<b>STATE OR COUNTRY</b> TX	<b>SHEETS DRAWINGS</b> 10	<b>TOTAL CLAIMS</b> 57	<b>INDEPENDENT CLAIMS</b> 6
<b>ADDRESS</b> SLATER & MATSIL, L.L.P. 17950 PRESTON RD, SUITE 1000 DALLAS, TX 75252-5793 UNITED STATES					
<b>TITLE</b> SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE					
<b>FILING FEE RECEIVED</b> 2578	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:		<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit		

<b>Index of Claims</b>  	<b>Application/Control No.</b> 12720147	<b>Applicant(s)/Patent Under Reexamination</b> ROZMAN ET AL.
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439

✓	<b>Rejected</b>
=	<b>Allowed</b>

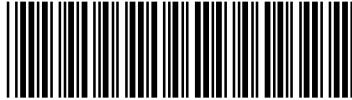
-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/29/2010	04/25/2011	10/20/2011	02/15/2012				
21	1	✓	✓	✓	=				
22	2	✓	✓	✓	=				
23	3	✓	✓	✓	=				
24	4	✓	✓	✓	=				
25	5	✓	✓	✓	=				
26	6	✓	✓	✓	=				
27	7	✓	✓	✓	=				
28	8	✓	✓	✓	=				
29	9	✓	✓	✓	=				
30	10	✓	✓	✓	=				
31	11	✓	✓	✓	=				
32	12	✓	✓	✓	=				
33	13	✓	✓	✓	=				
34	14	✓	✓	✓	=				
35	15	✓	✓	✓	=				
36	16	✓	✓	✓	=				
37	17	✓	✓	✓	=				
38	18	✓	✓	✓	=				
39	19	✓	✓	✓	=				
40	20	✓	✓	✓	=				
41	21	✓	✓	✓	=				
42	22	✓	✓	✓	=				
43	23	✓	✓	✓	=				
44	24	✓	✓	✓	=				
45	25	✓	✓	✓	=				
46	26	✓	✓	✓	=				
47	27	✓	✓	✓	=				
48	28	✓	✓	✓	=				
49	29	✓	✓	✓	=				
50	30	✓	✓	✓	=				
51	31	✓	✓	✓	=				
52	32	✓	✓	✓	=				
53	33	✓	✓	✓	=				
54	34	✓	✓	✓	=				
55	35	✓	✓	✓	=				
56	36	✓	✓	✓	=				

<b>Index of Claims</b>  	<b>Application/Control No.</b> 12720147	<b>Applicant(s)/Patent Under Reexamination</b> ROZMAN ET AL.
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>


N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/29/2010	04/25/2011	10/20/2011	02/15/2012				
57	37	✓	✓	✓	=				
58	38	✓	✓	✓	=				
59	39	✓	✓	✓	=				
60	40	✓	✓	✓	=				
61	41	✓	✓	✓	=				
62	42	✓	✓	✓	=				
63	43	✓	✓	✓	=				
64	44	✓	✓	✓	=				
65	45	✓	✓	✓	=				
66	46	✓	✓	✓	=				
67	47	✓	✓	✓	=				
68	48	✓	✓	✓	=				
69	49	✓	✓	✓	=				
70	50	✓	✓	✓	=				
71	51	✓	✓	✓	=				
72	52	✓	✓	✓	=				
73	53	✓	✓	✓	=				
74	54	✓	✓	✓	=				
75	55	✓	✓	✓	=				
76	56	✓	✓	✓	=				
77	57	✓	✓	✓	=				
78	58		✓	✓	=				
79	59		✓	✓	=				
80	60		✓	✓	=				
81	61		✓	✓	=				
82	62		✓	✓	=				
83	63		✓	✓	=				
84	64		✓	✓	=				
85	65		✓	✓	=				
86	66		✓	✓	=				
87	67		✓	✓	=				
88	68		✓	✓	=				
89	69		✓	✓	=				
90	70		✓	✓	=				
91	71		✓	✓	=				
92	72		✓	✓	=				



<b><i>Index of Claims</i></b>  	<b>Application/Control No.</b> 12720147	<b>Applicant(s)/Patent Under Reexamination</b> ROZMAN ET AL.
	<b>Examiner</b> Christian LaForgia	<b>Art Unit</b> 2439

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/29/2010	04/25/2011	10/20/2011	02/15/2012				
93	73		✓	✓	=				

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	((web with browser) same den\$4 with access with memory).clm.	US-PGPUB; USPAT	OR	ON	2012/02/15 09:12
S1	36	rozman-all\$.in.	US-PGPUB; USPAT	OR	OFF	2007/09/13 09:28
S2	2	cioffi-alf\$.in.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:49
S3	1	"6289462".pn.	US-PGPUB; USPAT	OR	OFF	2007/09/13 09:32
S4	10	((("7146640") or ("5835695") or ("6578140") or ("20050149933") or ("6892261") or ("6678712") or ("6957286") or ("6996828") or ("20040205755") or ("6697972")).PN.	US-PGPUB; USPAT	OR	OFF	2007/09/13 09:33
S5	5	("6578140").URPN.	USPAT	OR	OFF	2007/09/13 10:01
S6	1	(dual multiple) near (OS operat\$3 near systems) with (prevent\$3 stop\$4) with (virus trojan malicious malware)	US-PGPUB; USPAT	OR	ON	2007/09/13 10:06
S7	15	("6385721").URPN.	USPAT	OR	OFF	2007/09/13 10:03
S8	8	(dual multiple) near (OS operat\$3 near systems) with (virus trojan malicious malware)	US-PGPUB; USPAT	OR	ON	2007/09/13 13:58
S9	0	("2004/0039944").URPN.	USPAT	OR	OFF	2007/09/13 10:09
S10	35	((("5826013") or ("5978917") or ("6735700") or ("6663000") or ("6553377") or ("6216112") or ("4890098") or ("5555364") or ("5666030") or ("5995103") or ("5502808") or ("5280579") or ("5918039") or ("6480198") or ("6167522") or ("6199181") or ("6275938") or ("6351816") or ("6456554") or ("6658573") or ("6507904") or ("6633963") or ("6678825") or ("5751979") or ("20040054588") or ("20040034794") or ("20040006715") or ("20030177397") or ("20030097591") or ("20030023857") or ("20020066016") or ("20020174349") or ("6581162") or ("6134661") or ("6578140")).PN.	US-PGPUB; USPAT	OR	OFF	2007/09/13 10:13
S11	8	(US-20040039944-\$).did. or (US-7146640-\$ or US-6996828-\$ or US-	US-PGPUB;	OR	OFF	2007/09/13 10:28

		6678712-\$ or US-6578140-\$ or US-6385721-\$ or US-7260839-\$ or US-6199181-\$).did.	USPAT			
S12	0	S11 and network\$3 near (OS operat\$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 10:29
S13	8565	network\$3 near (OS operat\$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 10:29
S14	2	(dual multiple) near (OS operat\$3 near systems) same (display\$3) with both with (OS\$2 operat\$3 near systems)	US-PGPUB; USPAT	OR	ON	2007/09/13 11:55
S15	67	(dual multiple) near (OS operat\$3 near systems) same (display\$3) with (multiple) with (OS\$2 operat\$3 near systems)	US-PGPUB; USPAT	OR	ON	2007/09/13 11:55
S16	41	("5673403").URPN.	USPAT	OR	OFF	2007/09/13 12:12
S17	4565	(dual multiple) near (OS operat\$3 near systems)	US-PGPUB; USPAT	OR	ON	2007/09/13 14:49
S18	688	multi\$core near (processor cpu)	US-PGPUB; USPAT	OR	ON	2007/09/13 13:59
S19	37	S17 and S18	US-PGPUB; USPAT	OR	ON	2007/09/13 13:59
S20	18	S17 same S18	US-PGPUB; USPAT	OR	ON	2007/09/13 14:00
S21	4	S17 with S18	US-PGPUB; USPAT	OR	ON	2007/09/13 13:59
S22	14	S17 same S18 not S21	US-PGPUB; USPAT	OR	ON	2007/09/13 14:01
S23	19	S19 not S20	US-PGPUB; USPAT	OR	ON	2007/09/13 14:01
S24	665	(dual multiple) near (OS operat\$3 near systems) and (remov\$3 delet\$3) with (file program)	US-PGPUB; USPAT	OR	ON	2007/09/13 14:50
S25	1	(dual multiple) near (OS operat\$3 near systems) and (remov\$3 delet\$3) with (file program) with after near (run\$3 ran execut\$3)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:09
S26	17	(dual multiple) near (OS operat\$3 near systems) with encrypt\$3 \	US-PGPUB; USPAT	OR	ON	2007/09/13 15:09
S27	17	(dual multiple) near (OS operat\$3 near systems) with encrypt\$3	US-PGPUB; USPAT	OR	ON	2007/09/13 15:19
S28	36	(dual multiple) near (OS operat\$3 near systems) same encrypt\$3	US-PGPUB; USPAT	OR	ON	2007/09/13 15:19
S29	19	(dual multiple) near (OS operat\$3 near systems) same encrypt\$3 not S27	US-PGPUB; USPAT	OR	ON	2007/09/13 15:23

S30	676	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 not S28	US-PGPUB; USPAT	OR	ON	2007/09/13 15:33
S31	12	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (inter\$OS inter\$operat\$3 near system inter\$process\$2)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:35
S32	0	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (data information) with first near (OS operat\$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:38
S33	1	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with first near (OS operat\$3 near system)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:37
S34	9	(US-20040039944-\$.did. or (US-7146640-\$ or US-6996828-\$ or US-6678712-\$ or US-6578140-\$ or US-6385721-\$ or US-7260839-\$ or US-6199181-\$ or US-5673403-\$.did.	US-PGPUB; USPAT	OR	OFF	2007/09/13 15:37
S35	2	S34 and encrypt\$3	US-PGPUB; USPAT	OR	ON	2007/09/13 15:37
S36	81	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (OS operat\$3 near system) with (transfer communicat\$3 data)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:39
S37	6	(dual multiple) near (OS operat\$3 near systems) and encrypt\$3 with (OS operat\$3 near system) with (transfer communicat\$3)	US-PGPUB; USPAT	OR	ON	2007/09/13 15:39
S38	0	731/1.ccls.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:12
S39	2670	713/1.ccls.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:12
S40	1	"7027872".pn.	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:52
S41	0	"7027872".pn. and IMD with (authentikat\$3 authori\$6 verif\$7 valid\$5)	US-PGPUB; USPAT	OR	OFF	2007/09/13 16:52
S42	1	"7027872".pn. and (authentikat\$3 authori\$6 verif\$7 valid\$5)	US-PGPUB; USPAT	OR	OFF	2007/09/13 17:06
S43	1	"20050022020".pn.	US-PGPUB; USPAT	OR	OFF	2007/09/13 17:06
S44	1	"6192477".pn.	US-PGPUB; USPAT	OR	OFF	2008/02/19 13:13
S45	9	("6192477").URPN.	USPAT	OR	OFF	2008/02/19 13:14
S46	9	("6192477").URPN.	USPAT	OR	OFF	2008/06/16 16:15
S47	9	("6192477").URPN.	USPAT	OR	OFF	2008/06/16 16:15

S48	5	("6578140").URPN.	USPAT	OR	OFF	2008/08/18 14:31
S49	63	secure near3 process\$3 same insecure near3 process\$3	US- PGPUB; USPAT	OR	ON	2008/08/18 14:32
S50	1	secure near3 process\$3 same insecure near3 process\$3 with (internet e\$1mail)	US- PGPUB; USPAT	OR	ON	2008/08/18 14:32
S51	0	secure near3 processor and insecure near3 processor with (internet e\$1mail)	US- PGPUB; USPAT	OR	ON	2008/08/18 14:33
S52	9	("6192477").URPN.	USPAT	OR	OFF	2008/08/18 16:04
S53	1	common near (operat\$3 nears system OS) same protect\$3 near processor	US- PGPUB; USPAT	OR	ON	2008/08/18 16:33
S54	36	common near (operat\$3 nears system OS) and protect\$3 near processor	US- PGPUB; USPAT	OR	ON	2008/08/18 16:33
S55	0	(common near (operat\$3 nears system OS) and protect\$3 near processor).clm.	US- PGPUB; USPAT	OR	ON	2008/08/18 16:34
S56	1	"7484247".pn.	US- PGPUB; USPAT	OR	OFF	2010/12/21 13:22
S57	8	(("5673403") or ("5751979") or ("5974549") or ("5978917") or ("6091412") or ("6134661") or ("6397242") or ("6401134")).PN.	USPAT	OR	OFF	2010/12/21 13:27
S58	173	("5974549").URPN.	USPAT	OR	OFF	2010/12/21 13:29
S59	11	(("6433794") or ("6438600") or ("6492995") or ("6678825") or ("6691230") or ("6757685") or ("6836885") or ("7024555") or ("7139890") or ("7146640") or ("7260839")).PN.	USPAT	OR	OFF	2010/12/21 13:48
S60	3	(("7401230") or ("7421689") or ("7565522")).PN.	USPAT	OR	OFF	2010/12/21 13:51
S61	1291	eros	US- PGPUB; USPAT	OR	ON	2010/12/21 14:13
S62	12	eros and ("726" "713" "380").clas.	US- PGPUB; USPAT	OR	ON	2010/12/21 14:13
S63	0	eros with trust\$3 with window	US- PGPUB; USPAT	OR	ON	2010/12/21 14:14
S64	8	(("4890098") or ("5280579") or ("5502808") or ("5555364") or ("5666030") or ("5673403") or ("5751979") or ("5826013")).PN.	USPAT	OR	OFF	2010/12/21 14:54
S65	11	(("5918039") or ("5978917") or ("5995103") or ("6134661") or ("6167522") or ("6192477") or ("6199181") or ("6216112") or ("6275938") or ("6351816") or ("6385721")).PN.	USPAT	OR	OFF	2010/12/21 14:56

S66	11	(("6480198") or ("6507904") or ("6507948") or ("6546554") or ("6553377") or ("6578140") or ("6581162") or ("6633963") or ("6658573") or ("6663000") or ("6678825")).PN.	USPAT	OR	OFF	2010/12/21 14:58
S67	65	("6678825").URPN.	USPAT	OR	OFF	2010/12/21 14:58
S68	8	("6578140").URPN.	USPAT	OR	OFF	2010/12/21 15:09
S69	4	(("6735700") or ("6321337") or ("7146640") or ("7260839")).PN.	USPAT	OR	OFF	2010/12/21 15:10
S70	5	(("20020066016") or ("20020174349") or ("20030023857") or ("20030097591") or ("20030177397")).PN.	US-PGPUB	OR	OFF	2010/12/21 15:12
S71	6	(("20040006715") or ("20040034794") or ("20040039944") or ("20040054588") or ("20050240810") or ("20060004667")).PN.	US-PGPUB	OR	OFF	2010/12/21 15:13
S72	8	(("6880110") or ("7096381") or ("7577871") or ("7694328") or ("7373505") or ("7039801") or ("7596694") or ("7085928")).PN.	USPAT	OR	OFF	2010/12/21 15:18
S73	11	(("7181768") or ("7284274") or ("6804780") or ("7191469") or ("6505300") or ("7246374") or ("7062672") or ("7444412") or ("6772345") or ("6108715") or ("6873988")).PN.	USPAT	OR	OFF	2010/12/21 15:21
S74	1	"20030131152".pn.	US-PGPUB; USPAT	OR	OFF	2010/12/21 15:23
S75	4522	janus	US-PGPUB; USPAT	OR	OFF	2010/12/21 15:24
S76	1	"7484247".pn.	US-PGPUB; USPAT	OR	OFF	2010/12/21 15:47
S77	0	("7818808").URPN.	USPAT	OR	OFF	2010/12/22 06:08
S78	38	(execut\$3 run\$4) with (web HTML XML content) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:10
S79	2	(execut\$3 run\$4) with (plug\$in applet java\$script embed\$4 near executable) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:15
S80	2	(execut\$3 run\$4 render\$3) with (plug\$in applet java\$script embed\$4 near executable) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:15
S81	4	(execut\$3 run\$4 render\$3) with (malicious virus malware trojan spyware adware) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:17
S82	3	("2005/0005153").URPN.	USPAT	OR	OFF	2010/12/22 06:20

S83	2	(execut\$3 run\$4) with (plug\$in applet java\$script embed\$4 near (content executable)) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:21
S84	0	(execut\$3 run\$4 render\$3) with (separate isolat\$3) near (CPU processor microprocessor) same (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:21
S85	70	(execut\$3 run\$4 render\$3) with (separate isolat\$3) near (CPU processor microprocessor) and (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:21
S86	35	sandbox\$3 with (CPU processor microprocessor) same (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:29
S87	15	sandbox\$3 with (CPU processor microprocessor) and (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) not S86	US-PGPUB; USPAT	OR	ON	2010/12/22 06:30
S88	9	("20050283836" "20030051027" "20060259948" "20060191008" "20060080735" "6785732" "20050131868" "20010032205" "20060101514").pn.	US-PGPUB; USPAT	OR	ON	2010/12/22 06:33
S89	4	(web internet embed\$4) near (video audio content media) with (CPU processor microprocessor) same (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:37
S90	54	("5751979").URPN.	USPAT	OR	OFF	2010/12/22 06:39
S91	67	(web internet embed\$4) near (video audio content media) with (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:41
S92	3	(separate isolat\$3) near (CPU processor microprocessor) with (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:47
S93	5	(execut\$3 run\$4 render\$3) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) with (separate isolat\$3) near (CPU processor microprocessor)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:56
S94	0	((web internet embed\$4) near (content media video audio page site) web\$site web\$page) with (separate isolat\$3) near (CPU processor microprocessor) same (detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:57
S95	3	(separate isolat\$3) near (CPU processor microprocessor) with (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious	US-PGPUB; USPAT	OR	ON	2010/12/22 06:57

		virus malware trojan spyware adware)				
S96	1181	(CPU processor microprocessor) with (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:58
S97	15	(CPU processor microprocessor) with (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/22 06:58
S98	15	(CPU processor microprocessor) with (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) not S87	US-PGPUB; USPAT	OR	ON	2010/12/22 06:59
S99	0	(separate special\$4 isolat\$3 individual\$4) with (CPU processor microprocessor) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) not S87	US-PGPUB; USPAT	OR	ON	2010/12/22 07:03
S100	0	(separate special\$4 isolat\$3 individual\$4) with (CPU processor microprocessor) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3 prevent\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:03
S101	31	(CPU processor microprocessor) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3 prevent\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:04
S102	0	(execut\$3 run\$4 render\$3) with (separate isolat\$3) near (CPU processor microprocessor) with sandbox\$3	US-PGPUB; USPAT	OR	ON	2010/12/22 07:11
S103	0	(separate isolat\$3) near (CPU processor microprocessor) with sandbox\$3	US-PGPUB; USPAT	OR	ON	2010/12/22 07:11
S104	36	(CPU processor microprocessor) with sandbox\$3 with (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3 prevent\$3) with (malicious virus malware trojan spyware adware)	US-PGPUB; USPAT	OR	ON	2010/12/22 07:11
S105	11	("20050198692") or ("20050234856") or	US-	OR	OFF	2010/12/22



		("20060242166") or ("20060242709") or ("20060271835") or ("20080184105") or ("20080178302") or ("20080263358") or ("7562293") or ("7607172") or ("7698559").PN.	PGPUB; USPAT			07:14
S106	2	("2005/0198692").URPN.	USPAT	OR	OFF	2010/12/22 07:21
S107	8	("20050198692"   "5832208"   "6092194"   "6240530"   "6675174"   "6701440"   "7171691"   "7263561").PN.	US- PGPUB; USPAT; USOCR	OR	OFF	2010/12/22 07:22
S108	54	("5751979").URPN.	USPAT	OR	OFF	2010/12/22 07:24
S109	0	(divid\$3 division split\$4 spread\$3) with (CPU processor microprocessor) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US- PGPUB; USPAT	OR	ON	2010/12/22 07:41
S110	7	(divid\$3 division split\$4 spread\$3) with (CPU processor microprocessor) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) and (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	US- PGPUB; USPAT	OR	ON	2010/12/22 07:42
S111	183	(divid\$3 division split\$4 spread\$3) with (CPU processor microprocessor) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page)	US- PGPUB; USPAT	OR	ON	2010/12/22 07:43
S112	61	(execut\$3 run\$4 render\$3 display\$3 reproduc\$3) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page plug\$in script java\$script perl\$script) with (separate isolat\$3 individual second other) near (CPU processor microprocessor)	US- PGPUB; USPAT	OR	ON	2010/12/22 11:02
S113	9	(execut\$3 run\$4 render\$3 display\$3 reproduc\$3) with (suspicious malicious malware suspect\$2) with (separate isolat\$3 individual second other) near (CPU processor microprocessor)	US- PGPUB; USPAT	OR	ON	2010/12/22 14:18
S114	68	(execut\$3 run\$4 render\$3 display\$3 reproduc\$3) with (download\$2) with (separate isolat\$3 individual second other) near (CPU processor microprocessor)	US- PGPUB; USPAT	OR	ON	2010/12/22 14:20
S115	178	("5974549").URPN.	USPAT	OR	OFF	2010/12/28 14:11
S116	1	(CPU processor micro\$processor) with delegat\$3 same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	USPAT	OR	ON	2010/12/28 14:16
S117	7	(CPU processor micro\$processor) with	USPAT	OR	ON	2010/12/28

		delegat\$3 and (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)				14:17
S118	8	(CPU processor micro\$processor) with (transfer\$4 delegat\$3 assign\$4) with (task process application) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware)	USPAT	OR	ON	2010/12/28 14:18
S119	19	("6678712").URPN.	USPAT	OR	OFF	2010/12/28 14:21
S120	8	("6578140").URPN.	USPAT	OR	OFF	2010/12/28 14:27
S121	5	("20060107055"   "20080301670"   "6016546"   "6195587"   "6578140").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2010/12/28 14:27
S122	56	(virus anti\$virus) near (processor co\$processor)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:31
S123	3738	(CPU processor micro\$processor co\$processor video adj processor) with (display\$3 render\$3 reproduc\$4) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:34
S124	1	(CPU processor micro\$processor co\$processor video adj processor) with (display\$3 render\$3 reproduc\$4) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) same (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:35
S125	14	(CPU processor micro\$processor co\$processor video adj processor) with (display\$3 render\$3 reproduc\$4) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page) and (protect\$3 secur\$3 safe\$guard\$3 safe adj guard\$3 detect\$3 determin\$5 check\$3) with (malicious virus malware trojan spyware adware) with ((web internet embed\$4) near (content media video audio page site) web\$site web\$page)	US-PGPUB; USPAT	OR	ON	2010/12/28 14:35
S126	95	("6199181").URPN.	USPAT	OR	OFF	2010/12/28 14:38
S127	2	("2004/0039944").URPN.	USPAT	OR	OFF	2010/12/28 14:47
S128	14	("6192477").URPN.	USPAT	OR	OFF	2010/12/28 14:48
S129	1	"7146305".pn.	USPAT	OR	OFF	2010/12/28 14:50

S130	235	( "20010034847"   "20020032717"   "20020032793"   "20020032880"   "20020035698"   "20020083331"   "20020083334"   "20020138753"   "20020144156"   "20030037136"   "20030088791"   "20030212903"   "20040010718"   "4223380"   "4400769"   "4672609"   "4773028"   "4819234"   "4975950"   "5032979"   "5121345"   "5204966"   "5210704"   "5274824"   "5278901"   "5309562"   "5311593"   "5345595"   "5347450"   "5353393"   "5359659"   "5371852"   "5398196"   "5414833"   "5440723"   "5452442"   "5454074"   "5475839"   "5511184"   "5515508"   "5522026"   "5539659"   "5557742"   "5586260"   "5590331"   "5606668"   "5623600"   "5623601"   "5630061"   "5649095"   "5649185"   "5675711"   "5696486"   "5696822"   "5706210"   "5734697"   "5745692"   "5748098"   "5761504"   "5764887"   "5764890"   "5765030"   "5774727"   "5787177"   "5790799"   "5796942"   "5798706"   "5812763"   "5815574"   "5822517"   "5826013"   "5828833"   "5832208"   "5832211"   "5835726"   "5838903"   "5842002"   "5845067"   "5848233"   "5854916"   "5857191"   "5864665"   "5864803"   "5872978"   "5875296"   "5878420"   "5881236"   "5884033"   "5892903"   "5899999"   "5907834"   "5919257"   "5919258"   "5922051"   "5925126"   "5931946"   "5940591"   "5950012"   "5961644"   "5964839"   "5964889"   "5974237"   "5974457"   "5978917"   "5983270"   "5983348"   "5983350"   "5987606"   "5987610"   "5987611"   "5991856"   "5991881"   "5999711"   "5999723"   "6003132"   "6006016"   "6009467"   "6014645"   "6016553"   "6021510").PN. OR ("6026442"   "6029256"   "6035323"   "6035423"   "6041347"   "6052709"   "6061795"   "6067410"   "6070190"   "6070244"   "6073172"   "6081894"   "6085224"   "6088803"   "6088804"   "6092194"   "6094731"   "6098173"   "6104783"   "6108799"   "6118940"   "6119165"   "6119234"   "6122738"   "6144961"   "6154844"   "6161109"   "6167520"   "6173413"   "6185689"   "6195687"   "6199181"   "6205552"   "6226372"   "6230288"   "6266773"   "6266774"   "6271840"   "6272641"   "6275938"   "6275942"   "6278886"   "6279113"   "6282546"   "6298445"   "6301668"   "6314520"   "6314525"   "6321338"   "6324627"   "6324647"   "6324656"   "6338141"   "6347374"   "6353385"   "6357008"   "6377994"   "6396845"   "6397242"   "6397245"   "6405318"   "6405364"   "6408391"   "6415321"   "6429952"   "6434615"	US- PGPUB; USPAT; USOCR	OR	OFF	2010/12/28 14:50
------	-----	---	----------------------------------	----	-----	---------------------

		"6438600"   "6445822"   "6453345" "6453346"   "6460141"   "6463426" "6470449"   "6477585"   "6477648" "6477651"   "6484203"   "6487666" "6496858"   "6499107"   "6510523" "6517587"   "6519647"   "6519703" "6530024"   "6535227"   "6546493" "6563959"   "6574737"   "6578147" "6584454"   "6601190"   "6606744" "6618501"   "6628824"   "6647139" "6647400"   "6661904"   "6668082" "6668084"   "6681331"   "6691232" "6704874"   "6708212"   "6711127" "6711615"   "6718383"   "6721806" "6725377"   "6725378"   "6775780" "6792144"   "6792546"   "6816973" "6839850"   "6851057").PN.				
S131	12	("7146305").URPN.	USPAT	OR	OFF	2010/12/28 14:51
S132	5	restor\$3 with (file application program) with protect\$3 near image	US- PGPUB; USPAT	OR	ON	2010/12/28 17:07
S133	49	sub\$operat\$3 near system	US- PGPUB; USPAT	OR	ON	2010/12/29 15:43
S134	4503	(secure protect\$3 sand\$box\$3) with (web internet) near (browser viewer application)	US- PGPUB; USPAT	OR	ON	2010/12/30 11:06
S135	4100	(secure protect\$3 sand\$box\$3) with (web internet) adj (browser viewer application)	US- PGPUB; USPAT	OR	ON	2010/12/30 11:06
S136	4073	(secure protect\$3) with (web internet) adj (browser viewer application)	US- PGPUB; USPAT	OR	ON	2010/12/30 11:07
S137	15	(secure protect\$3) with (web internet) adj (browser viewer application) same sand\$box\$3 with (content media video audio embed\$4)	US- PGPUB; USPAT	OR	ON	2010/12/30 11:07
S138	19	(secure protect\$3) with (web internet) adj (browser viewer application) and sand\$box\$3 with (content media video audio embed\$4) not S137	US- PGPUB; USPAT	OR	ON	2010/12/30 11:09
S139	1	(US-20050149726-\$.did.	US- PGPUB	OR	OFF	2010/12/30 11:30
S140	1	S139 and scan\$4	US- PGPUB; USPAT	OR	ON	2010/12/30 11:30
S141	55	("2005/0149726").URPN.	USPAT	OR	OFF	2010/12/30 11:33
S142	0	S139 and (permission permitting permit)	USPAT	OR	ON	2010/12/30 11:40
S143	2	(US-20050149726-\$.did. or (US- 7146305-\$.did.	US- PGPUB; USPAT	OR	OFF	2010/12/30 12:18
S144	2	S143 and (cell\$4 mobile)	US- PGPUB; USPAT	OR	ON	2010/12/30 12:19
S145	258	list\$3 with block\$3 with (web\$site	US-	OR	ON	2010/12/30


		web\$page)	PGPUB; USPAT			12:24
S146	2	list\$3 with block\$3 with (web\$site web\$page) with (virus malware infection malicious trojan worm)	US- PGPUB; USPAT	OR	ON	2010/12/30 12:24
S147	4	list\$3 with block\$3 with (web\$site web\$page) same (virus malware infection malicious trojan worm)	US- PGPUB; USPAT	OR	ON	2010/12/30 12:25
S148	3	list\$3 with block\$3 with (web\$site web\$page) and 726/22-24.ccls.	US- PGPUB; USPAT	OR	ON	2010/12/30 12:25
S149	19	list\$3 with block\$3 with (web\$site web\$page) and "726".clas.	US- PGPUB; USPAT	OR	ON	2010/12/30 12:26
S150	10	(list\$3 with block\$3 black\$list\$3) with (web\$site web\$page) with (virus malware infection malicious trojan worm)	US- PGPUB; USPAT	OR	ON	2010/12/30 12:27
S151	16	(list\$3 with block\$3 black\$list\$3) with (web\$site web\$page) same (virus malware infection malicious trojan worm)	US- PGPUB; USPAT	OR	ON	2010/12/30 12:27
S152	6	(list\$3 with block\$3 black\$list\$3) with (web\$site web\$page) same (virus malware infection malicious trojan worm) not S150	US- PGPUB; USPAT	OR	ON	2010/12/30 12:27
S153	10	(list\$3 with block\$3 black\$list\$3) with (web\$site web\$page) and 726/22-24.ccls.	US- PGPUB; USPAT	OR	ON	2010/12/30 12:29
S154	7	(list\$3 with block\$3 black\$list\$3) with (web\$site web\$page) and 726/22-24.ccls. not S150	US- PGPUB; USPAT	OR	ON	2010/12/30 12:29
S155	10	(list\$3 with block\$3 black\$list\$3) with (web\$site web\$page) with (virus malware infect\$3 malicious trojan worm)	US- PGPUB; USPAT	OR	ON	2010/12/30 12:29
S156	43	(list\$3 with block\$3 black\$list\$3) with (web\$site web\$page) and ("726" "713").clas.	US- PGPUB; USPAT	OR	ON	2010/12/30 12:30
S157	34	(list\$3 with block\$3 black\$list\$3) with (web\$page web\$site site page) with (malicious malware infect\$3 virus) and ("726" "713").clas.	US- PGPUB; USPAT	OR	ON	2010/12/30 12:32
S158	37	((list\$3 table data\$base) with block\$3 black\$list\$3) with (web\$page web\$site site page) with (malicious malware infect\$3 virus) and ("726" "713").clas.	US- PGPUB; USPAT	OR	ON	2010/12/30 12:34
S159	3	((list\$3 table data\$base) with block\$3 black\$list\$3) with (web\$page web\$site site page) with (malicious malware infect\$3 virus) and ("726" "713").clas. not S157	US- PGPUB; USPAT	OR	ON	2010/12/30 12:34
S160	1	(US-7484247-\$).did.	USPAT	OR	OFF	2010/12/30 15:05
S161	1	"20040267929".pn.	US- PGPUB; USPAT	OR	OFF	2010/12/30 15:06
S162	1	(US-7484247-\$).did. and search\$3 near request\$3	USPAT	OR	ON	2010/12/30 15:06
S163	0	(secure protect\$3) with (web internet)	US-	OR	ON	2010/12/30

		adj (browser viewer application) same (prevent\$3 stop\$4) with search\$3 with (hack malicious\$2 hi\$jack)	PGPUB; USPAT			15:15
S164	1	(secure protect\$3) with (web internet) adj (browser viewer application) and (prevent\$3 stop\$4) with search\$3 with (hack malicious\$2 hi\$jack)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:15
S165	36	(prevent\$3 stop\$4) with search\$3 with (hack malicious\$2 hi\$jack)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:16
S166	58	search\$3 near (engine request) near4 (hack malicious\$2 hi\$jack)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:18
S167	59	search\$3 near (engine request) near4 (hack malicious\$2 hi\$jack\$3)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:19
S168	1	search\$3 near (engine request) near4 (hack malicious\$2 hi\$jack\$3) not S166	US-PGPUB; USPAT	OR	ON	2010/12/30 15:19
S169	3728010	prevent\$3 search\$3 near4 (hack malicious\$2 hi\$jack\$3)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:21
S170	15	prevent\$3 with search\$3 near4 (hack malicious\$2 hi\$jack\$3)	US-PGPUB; USPAT	OR	ON	2010/12/30 15:21
S171	59	("2005/0149726").URPN.	USPAT	OR	OFF	2011/03/03 16:07
S172	59	("2005/0149726").URPN.	USPAT	OR	OFF	2011/03/03 16:07
S173	2915	726/23-24.ccls.	US-PGPUB; USPAT	OR	OFF	2011/04/12 12:48
S174	5374	709/225.ccls.	US-PGPUB; USPAT	OR	OFF	2011/04/12 12:48
S175	93	S173 and S174	US-PGPUB; USPAT	OR	OFF	2011/04/12 12:48
S176	2	S173 and S174 and secure with browser	US-PGPUB; USPAT	OR	ON	2011/04/12 12:49
S177	911	713/151.ccls.	US-PGPUB; USPAT	OR	ON	2011/04/12 12:50
S178	422	713/152.ccls.	US-PGPUB; USPAT	OR	ON	2011/04/12 12:50
S179	25	S178 and S173	US-PGPUB; USPAT	OR	ON	2011/04/12 12:50
S180	1	"7039801".pn.	US-PGPUB; USPAT	OR	OFF	2011/04/12 12:59
S181	4	("7039801").URPN.	USPAT	OR	OFF	2011/04/12 13:38
S182	1	"20020002673".pn.	US-PGPUB;	OR	OFF	2011/04/12 13:38

			USPAT			
S183	5	("6049838"   "6108715"   "6330670"   "6434679"   "6487665").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2011/04/12 13:39
S184	10	("2002/0002673").URPN.	USPAT	OR	OFF	2011/04/12 13:40
S185	0	(block\$3 with modif\$7 with search near request\$3).clm.	US-PGPUB; USPAT	OR	ON	2011/04/12 13:51
S187	1	(US-7484247-\$).did.	USPAT	OR	OFF	2011/10/19 12:08
S188	1	S187 and browser	US-PGPUB; USPAT	OR	ON	2011/10/19 12:08
S189	5	((("6183366") or ("6285987") or ("20040199763") or ("6990630") or ("7676842")).PN.	US-PGPUB; USPAT	OR	OFF	2011/10/19 14:30
S190	3	("20020052809" "6756236" "7730318").pn.	US-PGPUB; USPAT	OR	OFF	2012/02/15 08:45
S191	2	("20040230794" "20050091661").pn.	US-PGPUB; USPAT	OR	OFF	2012/02/15 08:48
S192	122	713/151-152.ccls. and 726/22-24.ccls.	US-PGPUB; USPAT	OR	ON	2012/02/15 09:04

2/ 15/ 2012 9:13:22 AM

C:\Users\claforgia\Documents\EAST\Workspaces\12720147.wsp

<b>Search Notes</b>  	<b>Application/Control No.</b>  12720147	<b>Applicant(s)/Patent Under Reexamination</b>  ROZMAN ET AL.
	<b>Examiner</b>  Christian LaForgia	<b>Art Unit</b>  2439

SEARCHED			
Class	Subclass	Date	Examiner
none	none	12/29/10	clf
726	23-24	4/25/11	clf
713	152	4/25/11	clf
709	225	4/25/11	clf
none	none	10/19/11	clf
713	151,152	2/15/12	clf
726	22-24	2/15/12	clf

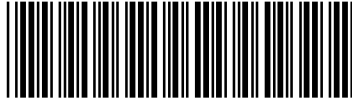
SEARCH NOTES			
Search Notes	Date	Examiner	
updated search for 10/913,609 (USPN 7,484,247)	12/29/10	clf	
updated EAST - see enclosed	4/25/11	clf	
updated EAST - see enclosed	10/19/11	clf	
updated EAST - see enclosed	2/15/12	clf	

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
	((web with browser) same den\$4 with access with memory).clm.	2/15/12	clf

	/Christian LaForgia/ Primary Examiner.Art Unit 2439
--	--





<b>Index of Claims</b>  	<b>Application/Control No.</b> 12720147	<b>Applicant(s)/Patent Under Reexamination</b> ROZMAN ET AL.
	<b>Examiner</b> CHRISTIAN LAFORGIA	<b>Art Unit</b> 2439

✓	<b>Rejected</b>
=	<b>Allowed</b>

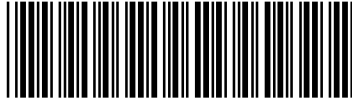
-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/29/2010	04/25/2011	10/20/2011	02/15/2012				
	1	✓	✓	✓	=				
	2	✓	✓	✓	=				
	3	✓	✓	✓	=				
	4	✓	✓	✓	=				
	5	✓	✓	✓	=				
	6	✓	✓	✓	=				
	7	✓	✓	✓	=				
	8	✓	✓	✓	=				
	9	✓	✓	✓	=				
	10	✓	✓	✓	=				
	11	✓	✓	✓	=				
	12	✓	✓	✓	=				
	13	✓	✓	✓	=				
	14	✓	✓	✓	=				
	15	✓	✓	✓	=				
	16	✓	✓	✓	=				
	17	✓	✓	✓	=				
	18	✓	✓	✓	=				
	19	✓	✓	✓	=				
	20	✓	✓	✓	=				
	21	✓	✓	✓	=				
	22	✓	✓	✓	=				
	23	✓	✓	✓	=				
	24	✓	✓	✓	=				
	25	✓	✓	✓	=				
	26	✓	✓	✓	=				
	27	✓	✓	✓	=				
	28	✓	✓	✓	=				
	29	✓	✓	✓	=				
	30	✓	✓	✓	=				
	31	✓	✓	✓	=				
	32	✓	✓	✓	=				
	33	✓	✓	✓	=				
	34	✓	✓	✓	=				
	35	✓	✓	✓	=				
	36	✓	✓	✓	=				

<b><i>Index of Claims</i></b>  	<b>Application/Control No.</b> 12720147	<b>Applicant(s)/Patent Under Reexamination</b> ROZMAN ET AL.
	<b>Examiner</b> CHRISTIAN LAFORGIA	<b>Art Unit</b> 2439

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/29/2010	04/25/2011	10/20/2011	02/15/2012				
	37	✓	✓	✓	=				
	38	✓	✓	✓	=				
	39	✓	✓	✓	=				
	40	✓	✓	✓	=				
	41	✓	✓	✓	=				
	42	✓	✓	✓	=				
	43	✓	✓	✓	=				
	44	✓	✓	✓	=				
	45	✓	✓	✓	=				
	46	✓	✓	✓	=				
	47	✓	✓	✓	=				
	48	✓	✓	✓	=				
	49	✓	✓	✓	=				
	50	✓	✓	✓	=				
	51	✓	✓	✓	=				
	52	✓	✓	✓	=				
	53	✓	✓	✓	=				
	54	✓	✓	✓	=				
	55	✓	✓	✓	=				
	56	✓	✓	✓	=				
	57	✓	✓	✓	=				
	58		✓	✓	=				
	59		✓	✓	=				
	60		✓	✓	=				
	61		✓	✓	=				
	62		✓	✓	=				
	63		✓	✓	=				
	64		✓	✓	=				
	65		✓	✓	=				
	66		✓	✓	=				
	67		✓	✓	=				
	68		✓	✓	=				
	69		✓	✓	=				
	70		✓	✓	=				
	71		✓	✓	=				
	72		✓	✓	=				

<b><i>Index of Claims</i></b>  	<b>Application/Control No.</b> 12720147	<b>Applicant(s)/Patent Under Reexamination</b> ROZMAN ET AL.
	<b>Examiner</b> CHRISTIAN LAFORGIA	<b>Art Unit</b> 2439

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

Claims renumbered in the same order as presented by applicant
  CPA
  T.D.
  R.1.47

CLAIM		DATE							
Final	Original	12/29/2010	04/25/2011	10/20/2011	02/15/2012				
	73		✓	✓	=				

**PART B - FEE(S) TRANSMITTAL**

Complete and send this form, together with applicable fee(s), to: **Mail** Mail Stop ISSUE FEE  
**Commissioner for Patents**  
**P.O. Box 1450**  
**Alexandria, Virginia 22313-1450**  
**or Fax** (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

23962 7590 05/14/2012  
**SLATER & MATSIL, L.L.P.**  
 Ira Matsil  
 17950 PRESTON RD, SUITE 1000  
 DALLAS, TX 75252-5793

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/720,147	03/09/2010	Allen F. Rozman	ARAC-01RE1	8473

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	\$870	\$0	\$0	\$870	08/14/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
LAFORGIA, CHRISTIAN A	2439	726-024000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

"Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a **Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

Slater & Matsil, L.L.P.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent):  Individual  Corporation or other private group entity  Government

4a. The following fee(s) are submitted:

Issue Fee

Publication Fee (No small entity discount permitted)

Advance Order - # of Copies \_\_\_\_\_

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

A check is enclosed.

Payment by credit card. Form PTO-2038 is attached.

The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number **50-1065** (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.  b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature Glenn W. Boisbrun  
 Digitally signed by Glenn W. Boisbrun  
 DN: cn=Glenn W. Boisbrun, o=Glenn W. Boisbrun, email=glennboisbrun@slater-matsil.com, c=US  
 1986-2012 05/14/2012 09:07

Typed or printed name Glenn W. Boisbrun

Date May 23, 2012  
 Registration No. 39,615

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	12720147
<b>Filing Date:</b>	09-Mar-2010
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Filer:</b>	Glenn W. Boisbrun/Sherry Colgrove
<b>Attorney Docket Number:</b>	ARAC-01RE1

Filed as Small Entity

### Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
Utility Appl issue fee	2501	1	870	870

**Extension-of-Time:**

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>870</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	12851215
<b>Application Number:</b>	12720147
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	8473
<b>Title of Invention:</b>	SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE
<b>First Named Inventor/Applicant Name:</b>	Allen F. Rozman
<b>Customer Number:</b>	25962
<b>Filer:</b>	Glenn W. Boisbrun/Sherry Colgrove
<b>Filer Authorized By:</b>	Glenn W. Boisbrun
<b>Attorney Docket Number:</b>	ARAC-01RE1
<b>Receipt Date:</b>	23-MAY-2012
<b>Filing Date:</b>	09-MAR-2010
<b>Time Stamp:</b>	18:34:17
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$870
RAM confirmation Number	7460
Deposit Account	501065
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)



Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	ARAC-01RE1_Part_B_Fee_Transmittal.pdf	197082 ad95a1cb99624251c707d24d964c4a3a64dae3d2	no	1

### Warnings:

### Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30546 9b61fc1c4fd6338f823f11da05d39faa64ae0d61	no	2
---	----------------------	--------------	---	----	---

### Warnings:

### Information:

**Total Files Size (in bytes):** 227628

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

#### **New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

#### **National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

#### **New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/720,147	07/17/2012	RE43528	ARAC-01RE1	8473

25962 7590 06/27/2012  
SLATER & MATSIL, L.L.P.  
Ira Matsil  
17950 PRESTON RD, SUITE 1000  
DALLAS, TX 75252-5793

**ISSUE NOTIFICATION**

The projected patent number and issue date are specified above.

**Determination of Patent Term Extension or Adjustment under 35 U.S.C. 154 (b)**

A reissue patent is for "the unexpired part of the term of the original patent." See 35 U.S.C. 251. Accordingly, the above-identified reissue application is not eligible for Patent Term Extension or Adjustment under 35 U.S.C. 154(b).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Allen F. Rozman, Garland, TX;  
Alfonso J. Cioffi, Murphy, TX;

AO 120 (Rev. 08/10)

TO: <b>Mail Stop 8</b> <b>Director of the U.S. Patent and Trademark Office</b> <b>P.O. Box 1450</b> <b>Alexandria, VA 22313-1450</b>	<b>REPORT ON THE</b> <b>FILING OR DETERMINATION OF AN</b> <b>ACTION REGARDING A PATENT OR</b> <b>TRADEMARK</b>
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas, Marshall Division on the following

Trademarks or  Patents. (  the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 2:13-cv-103	DATE FILED 2/5/2013	U.S. DISTRICT COURT Eastern District of Texas, Marshall Division
PLAINTIFF ALFONSO CIOFFI, MELANIE ROZMAN, MEGAN ROZMAN, and MORGAN ROZMAN		DEFENDANT Google, Inc.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 RE43,103	1/10/2012	Allen F. Rozman and Alfonso C. Cioffi
2 RE43,500	7/3/2012	Allen F. Rozman and Alfonso C. Cioffi
3 RE43,528	7/17/2012	Allen F. Rozman and Alfonso C. Cioffi
4 RE43,529	7/17/2012	Allen F. Rozman and Alfonso C. Cioffi
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading		
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK	
1			
2			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT
--------------------

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director    Copy 3—Upon termination of action, mail this copy to Director  
 Copy 2—Upon filing document adding patent(s), mail this copy to Director    Copy 4—Case file copy