INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2004/000409

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 101 376 A (NOGUCHI KOUKI ET AL) 31 March 1992 (1992-03-31) abstract column 1, line 31 - column 3, line 12 figures 1,10,12	3-5,18, 23,25
A	US 5 452 451 A (AKIZAWA MITSURU ET AL) 19 September 1995 (1995-09-19) the whole document	3-5,18, 23,25

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US2004/000409

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6212625 B1	03-04-2001	NONE	
US 6327508 B1	04-12-2001	NONE	
EP 0488297 A	03-06-1992	JP 2960533 B2	06-10-1999
		JP 4205174 A	27-07-1992
		DE 69131954 D1	09-03-2000
		DE 69131954 T2	05-10-2000
		EP 0488297 A2	03-06-1992
		US 5497488 A	05-03-1996
US 5101376 A	31-03-1992	JP 3130994 A	04-06-1991
		KR 159941 B1	01-02-1999
		US 5036486 A	30-07-1991
US 5452451 A	19-09-1995	JP 2825009 B2	18-11-1998
		JP 3017780 A	25-01-1991
		JP 2880199 B2	05-04-1999
		JP 3131969 A	05-06-1991
		US 5497488 A	05-03-1996

SOPHOS
EXHIBIT 1004 - PAGE 0318

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **08-263447**
(43)Date of publication of application : **11.10.1996**

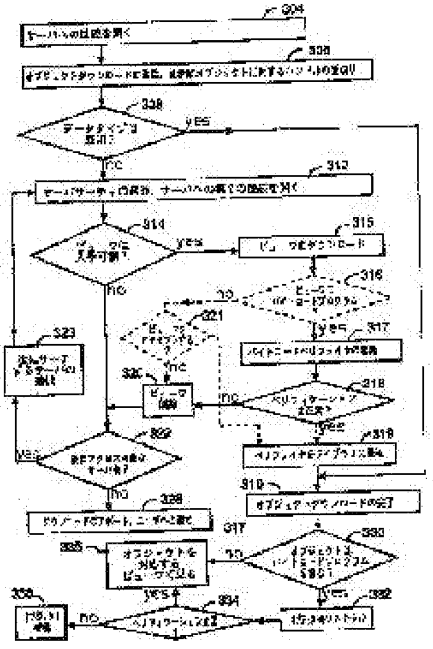
(51)Int.Cl. G06F 15/16
G06F 9/445
G06F 13/00

(21)Application number : **07-349164**
(22)Date of filing : **20.12.1995**

(71)Applicant : **SUN MICROSYST INC**
(72)Inventor : **GOSLING JAMES A**

(30)Priority
Priority number : **94 359884** Priority date : **20.12.1994** Priority country : **US**

(54) DISTRIBUTED COMPUTER SYSTEM AND OPERATION METHOD THEREFOR



(57)Abstract:
PROBLEM TO BE SOLVED: To provide a distributed computer system provided with a computer for automatically clown-loading the viewer of an object to be referred to and verifying the maintainability of a loaded program and the operation method.
SOLUTION: At the time of loading data (object) stored in another server or the like through a network and referring to them, the viewer corresponding to the object is automatically searched, and in the case that the appropriate viewer is found in the other server or the like, verification is performed so as to confirm the maintainability before activating the viewer. Especially, importance is placed in the verification relating to the use of a stack and a data type to the program written in a byte code language.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 11/00, 17/00	A1	**(11) International Publication Number:** **WO 95/33237** **(43) International Publication Date:** 7 December 1995 (07.12.95)

(21) International Application Number: PCT/US95/06659

(22) International Filing Date: 30 May 1995 (30.05.95)

(30) Priority Data:
08/252,622 1 June 1994 (01.06.94) US

(71) Applicant: QUANTUM LEAP INNOVATIONS INC. [US/US]; 410 Briarcliff Road, Briarcliff Manor, NY 10510 (US).

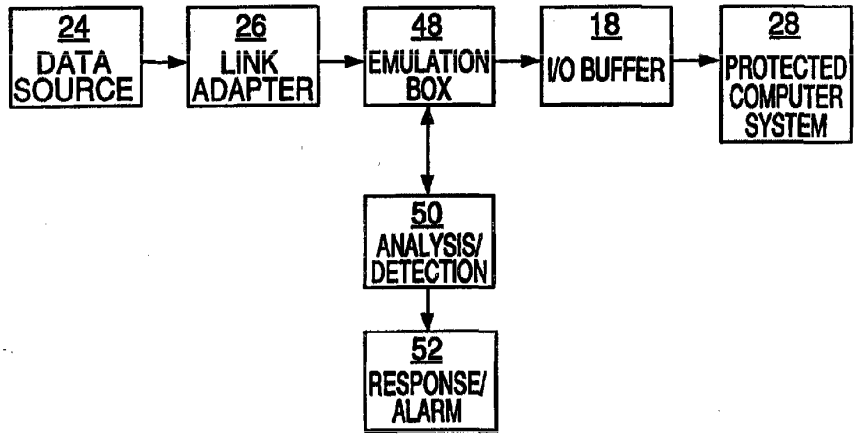
(72) Inventors: SCHNURER, John; P.O. Box 446, Yellow Springs, OH 45387 (US). KLEMMER, Timothy, J.; 410 Briarcliff Road, Briarcliff Manor, NY 10510 (US).

(74) Agent: AMARAL, Anthony, Jr.; Reid & Priest L.L.P., 40 West 57th Street, New York, NY 10019 (US).

(81) Designated States: CA, CN, DE, GB, JP, MX, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: COMPUTER VIRUS TRAP



(57) Abstract

A computer virus trapping device (10) is described that detects and eliminates computer viruses before they can enter a computer system and wreck havoc on its files, peripherals, etc. The trapping device (10) creates a virtual world that simulates the host computer system (28) intended by the virus to infect. The environment is made as friendly as possible to fool a computer virus into thinking it is present on the host (28), its intended target system. Within this virtual world, the virus is encouraged to perform its intended activity. The invention is able to detect any disruptive behaviour occurring within this simulated host computer system. It is further able to remove (52) the virus from the data stream before it is delivered to the host (28) and/or take any action previously instructed by a user (38).

SOPHOS
EXHIBIT 1004 - PAGE 0320

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

SOPHOS
EXHIBIT 1004 - PAGE 0321

COMPUTER VIRUS TRAP

BACKGROUND OF THE INVENTION

The computer virus problem that exists today had its beginnings sometime in the late 1980s. At that time computer viruses were a novelty and plagued mainly DOS and Macintosh computers. Today, almost every Fortune 500 company has experienced computer viruses with the current rate being about one virus incident every 2 to 3 months.

The term computer virus is applied in common and legal usage to software, code, code blocks, code elements and code segments which perform certain functions in the digital computer environment. Code is intended to mean the digital instructions which the computer responds to. Non damaging or legitimate software, code, code blocks, code segments and code elements that serve a useful purpose would not be considered a virus.

Computer viruses have been known to cause physical harm to computer hardware in addition to erasing and destroying data. While rare, there have been cases of viruses that have made calls to disk drive heads actually scoring the media; still others have been discovered that ramped up the scan rate on a monitor causing failure. Most viruses do not, however, intentionally cause explicit physical harm and they are discovered before they are triggered to cause damage to data and files. However, it is after discovery that the real cost of viruses becomes apparent in connection with their detection and removal. In an average computer site this might entail searching 1000 PCs and 35,000 diskettes. If the software engineer misses even one instance of the virus, other computers will be re-infected and the clean up search must be repeated all over again.

A common misconception is that there are good viruses and bad viruses. Some viruses are claimed to be benign because they do not have a malicious

SOPHOS
EXHIBIT 1004 - PAGE 0322

trigger event and cannot do intentional harm. However, this misses the point that the problems computer viruses cause are mainly due to the trigger events. It is a fact that computer viruses replicate. This by itself is harmful because it necessitates a search to clean up all instances of the viruses in a computer installation.

The damage caused by viruses, not so much due to erased files or data, but in the cost of detection, removal and also the accompanying lowered worker productivity can be very high. It has been calculated that the average computer site will spend on the order of about $250,000 on a computer virus cleanup. It has been estimated that computer viruses will cost U.S. computer users over a billion dollars in 1994 alone.

The problem will grow exponentially due to the advent of the Information Super Highway. The increased connectivity among individuals, companies and government will allow a computer virus to create havoc. Currently disjoint computer systems that perform various functions that we take for granted today, such as, banking, telecommunications, radio, information databases, libraries and credit might meld together in the future. Thus, computer viruses, unchecked, could have a crippling effect on our society.

A virus can only cause trouble when it enters a system and finds a location on which to act. In a general sense, the virus must perform an intended function or a function the user or operator did not intend, expect, compensate for or otherwise protect against. Some examples of malicious virus activity are: changing names of files making it difficult for the user to access the files, moving a file to a new location, deleting files, interfering with working programs (i.e. causing all the words on a screen to fall to the bottom of the screen in a heap), replicating themselves and clogging up the system making it nonfunctional or waiting for a predetermined time period or after a certain number of toggle operations such as boot, access, cursor movements, mouse clicks, etc. before acting.

SOPHOS
EXHIBIT 1004 - PAGE 0323

More felonious type viruses are those that have been released to cause ruin or impairment of a system for the purposes of sabotage, espionage, financial gain or to impair a competing business. Some examples include: creating a trap door which allows access to an unauthorized user for any purpose such as espionage, dumping files or erasure, navigation programs which find routes into systems, password cracking programs, modifying the executable segment of legitimate programs and attaching themselves to a code block and travel to another site.

In addition to traditional PCs and networks being vulnerable to virus infections, embedded control systems often used in industrial process control settings are also vulnerable. These systems control machinery, motors, industrial robots and process data from sensors. Because embedded systems are vulnerable to viruses just as PCs are, the results are potentially quite damaging. The smooth flow of a factory or assembly line could be devastated by a virus' uncontrolled behavior.

There are many possible ways for a virus to act on a computer system. All computers go through a boot procedure in which the Basic Input Output System (BIOS) and/or other resident system tools perform a variety of startup tasks such as, finding drives, testing memory and the system, initiating system files, loading DOS or other Operating System (OS) and bringing up an initial startup program. The system performs certain housekeeping tasks such as establishing various links among other functions. A computer system of any utility is complex enough that someone writing a virus has a myriad of opportunities and possibilities in which to cause trouble and interfere with the proper operation of the system.

The most common solution to the virus problem is to employ anti-virus software that scans, detects and eliminates viruses from computer systems. These programs work by searching a storage medium such as a hard disk drive or floppy diskette for known patterns of various viruses. However, there are

SOPHOS
EXHIBIT 1004 - PAGE 0324

problems associated with this method of virus elimination. The software can only scan for known viruses which have an identifiable pattern that can be detected using repetitive string searches. To protect against new viruses frequent upgrades must be distributed. In addition, for the program to detect a virus it must already have infected that computer. The virus might have done some damage or even replicated itself and spread before it is detected. Also, the program must be run often to provide effective protection against viruses especially on systems where programs and data are transferred frequently between computers via diskettes.

In addition further liabilities, pratfalls and limitations to the current breed of anti-virus software solutions exist. This software breaks down into 3 categories: scanners, monitors, CRC's. Scanners as previously mentioned work off of databases of known strings. These databases are in constant need of updates. Monitors are memory resident programs monitoring the computer for questionable behavior. Monitors suffer from high rates of false positives, and they occupy and take a large portion of the limited conventional memory of a PC. CRC's are error checking programs that generate a unique "signature" in the form of a 2-byte number for each and every file to be protected. CRC programs either place the "signature" in the file itself or in a separate file. CRC programs suffer from the fact that they are easy to identify and thus easily tricked into recreating a "signature" for an infected file. Further, Scanners & Monitors & CRC programs must be run on the PC in question. Often this is a time consuming chore. These programs usually must have full control of the PC to operate further inconveniencing the user because he must wait for the scanner to finish before he can begin his normal work. The other critical concept is that the anti-virus software is run on the PC in question. It is subject to the limitations and liabilities of the operating system and may already be running on an infected PC without knowing it. The invention takes a unique approach by performing

SOPHOS
EXHIBIT 1004 - PAGE 0325

its logic outside of the PC, not inconveniencing the user and is more effective because the invention's hardware guarantees a clean uninfected start.

Another possible solution is to increase computer security to the point where viruses cannot enter the system. Login/password control and encryption do not effect computer viruses. With encryption, detection and elimination is made more difficult because the virus along with good data is encrypted, only becoming decrypted when it attempts to replicate. Clearly, this is quite burdensome and expensive to implement.

Another possible solution is to avoid computer bulletin boards, both the commercial type such as, Compuserve, Prodigy, the Internet and Usenet, and the private, local, small type. However, this will not prevent viruses from spreading because most viruses do not result from software or data downloaded from information databases or computer bulletin boards. The operators of both commercial on-line services and private bulletin boards are very careful to keep viruses off their systems. They are constantly searching and scanning anything that is uploaded to their systems before making it available to their subscribers. In addition, most computer viruses of the boot track type do not spread through download data or software. The majority of viruses are spread through diskettes. There are known instances of commercial software being distributed after being infected by a virus. There are known instances of viruses being distributed unwittingly by diskette manufacturers on blank diskettes. There are no rules for which diskettes are more likely to be free from viruses.

Thus, there is a long felt need for a device that can search for, detect and eliminate viruses before they ever enter into a computer system that is transparent to a user and effective against all viruses in existence today and those not yet created.

SUMMARY OF THE INVENTION

One characteristic of almost all viruses is that on their own they are not capable of crossing from one computer OS to another. This is because different

SOPHOS
EXHIBIT 1004 - PAGE 0326

computer systems in use today have different internal instructions or command sets. The language perfectly acceptable and intelligible to one OS does not have any correlation to another. An analogy to humans would be two people speaking different languages not being able to communicate. Although there might exist identical words present in both languages it is statistically very unlikely for a misinterpreted or cross over string of words or set of computer instructions (i.e. a virus) to convey a significant amount of information or be able to effectively execute a series of instructions. It is even more unlikely for this misinterpreted or cross over string of words or series of instructions to migrate from one language or system to another language or system and still be able to convey any useful information or execute a series of commands.

The present invention utilizes this characteristic of viruses to create an impenetrable barrier through which a virus cannot escape. The use of a foreign operating system guarantees the invention a high degree of safety and impenetrability. While the inventors recognize that such invention can be built without the use of a foreign operating system, such a version of the invention would lack any creditable degree of security. In addition, without the use of a foreign operating system the invention itself risks contamination. A foreign operating system different from the one being protected is introduced into the data stream before the data arrives at the computer system to be protected. To illustrate: if a program written for DOS will not run as intended on a Macintosh neither will a virus. A foreign operating system in order to complete its operation must provide an emulation of the target computer operating system (disk drives, memory configuration, ports, etc.). The virus is therefor fooled into thinking it is resident on the target computer system it was intending to infect. It is here, while the virus is resident within the emulated target operating system, that the virus is encouraged to infect files, destroy data and wreak havoc. It is here that the invention diverges from all other strategies in virus-detection and prevention. All other strategies are defensive in nature: they mark

SOPHOS
EXHIBIT 1004 - PAGE 0327

files to detect unwarranted changes, they scan for unintended behavior in an attempt to prevent the virus from performing its damage. The present invention takes an offensive strategy by encouraging the virus to infect and destroy files.

The most critical behavior of a virus that computer users to prevent is the virus ability to replicate. Once a virus has erased a file, made a hard drive inoperable, it is detected. Once the virus has done anything considered malicious, it usually is detected. At this point anti-virus software and hardware must be brought in and run to detect and clean files. Prior to its performing this malicious act, a virus must replicate. If it does not replicate, it cannot grow and stay alive. If it has the ability to replicate, it can travel from PC to floppy to PC to network, etc. It is this behavior of viruses to replicate that the present invention preys on. The virus is encouraged to act within this cross platform generated emulation so that it can be detected. It is this use of cross platform technology and offensive strategy that allows a virus to be detected at any level before any damage occurs to the protected system. It is in the emulation that the invention can detect the virus and in the use of transplatform logic/environment that it can safely contain the virus. Where the virus can get around DOS or MAC scanners or Operating System or BIOS, it cannot infiltrate and contaminate the foreign operating system.

A foreign operating system is chosen based on its ability to monitor and watch any emulations, and for being able to manipulate elements within the emulation (files, falsifying BIOS information, creating sham peripherals), and for the sheer speed and computational horsepower.

The inventors recognize that it can be done without a transplatform, but it will be slow and absolutely unsafe. The use of a foreign operating system can be likened to the use of lead walls and glass walls and mechanical arms used by people manipulating radioactive materials in labs. While it is certainly possible to pick up radioactivity with one's bare hands, it is not highly recommended or is

SOPHOS
EXHIBIT 1004 - PAGE 0328

it safe. While the invention can be had without the use of a foreign operating system, it is not highly recommended nor is it safe.

A primary object of the present invention is to provide a virus detection system to detect and eliminate viruses at their most basic level by simulating the host's environment by creating a virtual world to fool the virus into thinking it is resident on the host so as to allow disruptive behavior to be detected and the virus destroyed without harm to the host.

Another object of the present invention is to provide a virus detection system able to detect and trap viruses at any level using in a way other than performing string searches through memory or files to detect viruses.

Yet another object of the present invention is to provide a virus detection system able to detect as of yet unknown viruses thereby obviating the need for software updates to keep the detection device current.

Still another object of the present invention is to minimize the down time of the host computer system in the event a virus is detected.

Still another object of the invention is to record at the user's discretion the virus to another media for transferal to virus analysis groups. The object is to feed the virus to an internal analysis to compare against a know, previously acquired attempt, such as a trapdoor or file change, or industrial espionage or sabotage code, etc.

Still another object is to record from which incoming source the virus came, i.e., modem, which digiboard channel, internet, Compuserve, LAN station/Userid, WAN line, etc.

Another object is to alert system administration of the attack.

BRIEF DESCRIPTION OF THE DRAWINGS

Serving to illustrate exemplary embodiments of the invention are the drawings of which:

Fig 1 is a high level functional block diagram of the preferred embodiment of the present invention.

SOPHOS
EXHIBIT 1004 - PAGE 0329

Fig. 2 is a functional block diagram of the preferred embodiment of the present invention;

Fig. 3 is a functional block diagram showing the application of the present invention in a local area networking environment;

Fig. 4 is a functional block diagram showing the application of the present invention in a telecommunications networking environment;

Fig. 5 is a high level software logic diagram showing the operating steps of the present invention;

Figs. 6A to 6C together comprise a high level flow chart of the operating steps of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

In order to afford a complete understanding of the invention and an appreciation of its advantages, a description of a preferred embodiment of the present invention in a typical operating environment is presented below.

Operating on the principle that a virus cannot cross operating systems, the present invention creates a virtual world for a potential virus. An OS that emulates the system to be protected provides a friendly familiar environment for the virus. The virus is encouraged to act in this virtual world created for it. The results of the virus' disruptive behavior can be detected and consequently the virus can be flagged and eliminated or stored and further analyzed. This scheme is based on the assumptions that almost all viruses are executable in nature, no user would try to purposely communicate a destructive virus to another and that it is possible to identify executable instructions in an environment where the instruction cannot possibly operate.

Shown in Figures 1 and 2 are functional block diagrams of the virus trapping device 10. The Central Processing Unit (CPU) 12 can be any computing device (i.e. Intel, Motorola, Paramid, National Semincondutor or Texas Instruments microprocessor, multiple chip set CPUs, board level CPUs, etc.). The Transputer is particularly well suited because almost all PCs in use

SOPHOS
EXHIBIT 1004 - PAGE 0330

today employ CPUs other than the Transputer. A guide to the application and programming of the Transputer can be found in The Transputer Handbook, by Mark Hopkins, copyright 1989 INMOS Ltd. and The Transputer Databook, by Mark Hopkins, 3rd Edition copyright 1992 INMOS Ltd. Italy. As a typical microprocessor circuit design, EPROM 14 holds the operating software for the CPU 12. RAM 16 provides a temporary storage facility for the CPU 12 to execute the virus detection software. Link adapters 20 provide physical connections to interface the virus trapping device 10 to the outside world. The trap device 10 is not limited to two link adapters, any number could be implemented to handle a multitude of input data streams. The device 10 reads an incoming data stream from one or more outside sources. An example of a communication link 24 are a Local Area Network (LAN) (i.e. Novell), Wide Area Network (WAN) (i.e. networked LANs), the telephone network (i.e. Modems), radio frequency (RF) type cellular network or some type of data storage device (i.e. floppy diskette, hard disk, tape, CD-ROM, magneto-optical, etc.). The communication link 24 provides an incoming data stream for the device 10 to operate on. Diskettes are commonly used to transfer data and programs from one computer to another, thus making it a common entry point into the system for viruses. An input/output (I/O) interface 18 provides a means for the virus trapping device 10 to communicate with the computer system being protected 28.

The application of the virus trapping device 10 in a typical operating environment is shown in Figure 3. The file server 42 is the computer system to be protected. The virus trapping device 10 is placed in the data stream that connects the filer server 42 to other workstations 38. The hubs 40 serve to connect the workstations 38 into a LAN and the modems 36 serve to connect remote workstations 38 to the file server 42. In this scenario, all traffic to and from the file server 42 is monitored for viruses by the trap 10.

SOPHOS
EXHIBIT 1004 - PAGE 0331

Another application of the trapping device 10 is shown in Figure 4. In this scenario, data traffic passing through the telecommunications network 34 is protected from viruses. A user might have a mainframe file server 30 at a remote site connected to the telephone network 34. Nodes 32 located in the telephone company's central offices perform access and cross connect functions for customers' data traffic. To prevent the spread of a virus through the network, the trapping device 10 is placed in front of each node 32. Data traffic between workstations 38 connected to the telephone network 34 via modems 36 and the mainframe file server 30 is constantly checked for viruses because the traffic must pass through the virus trapping device 10.

Operation of the virus trapping device 10 is as follows. The trapping device 10 monitors the data stream that enters from the outside world, such as from the communications link 24. All data is treated as data whether it is actually data (i.e. data files) or instructions (i.e. executables) as it passes over the link 24. At this point the actual instructions have not been executed but rather they are in the process of being transmitted for execution. While in this state of transmission, emulation means 48, controlled by the CPU 12, provide a friendly environment for a potential virus. The data is put into the emulation chamber 48 where the virus is fooled into acting as if it were really present on the host system. It is desired that any disruptive behavior the virus is capable of displaying take place in emulation chamber 48 such as replicating, attacking another program or destroying data. In this virtual world the virus has complete access to its environment. It is at this point that analysis and detection means 50 controlled by the CPU 12 catches the virus in the act of self replication and prevents it from infecting the host system. The virus cannot escape the emulation box 48 because the box exists in a foreign operating environment with no access to critical files, keyboard, screen, etc. Access to the real world is completely blocked.

SOPHOS
EXHIBIT 1004 - PAGE 0332

Upon startup of the trapping device 10, the emulation software is read from EPROM 14 and executed. When a user turns on his workstation 38, a connection is established between the workstation 38 and the file server 30 (or 42). A connection session is created in the RAM 16 of the CPU 12. In like fashion, a session is created for each user.

As the user at a workstation 38 runs commands and moves file about, data is ultimately written to and read from the file server 30. The trapping device 10 splits the data into two paths. One path connects directly to the protected computer system 28 without modification. Data over the other path is written into the emulation box or virtual world created for each user. The write is performed in this box just as it would have been performed on the file server 30, protected computer 28 or workstation 38. Changes in data and time are simulated to trigger time sensitive viruses, fooling then as to the actual data and time. If the environment changes, it is checked to determine whether simply data was written or whether executable code was written.

Once the executable in inside the emulation box, a Cyclic Redundancy Check (CRC) is made of the Interrupt Request table (IRQ). Also, CRCs are generated on all files that are placed in the emulation box. The CRC is an error detection and correction code widely used in the computer and engineering fields. Other aspects of the environment, such as available memory, are saved too. All information saved is stored outside of the emulation box where it cannot be altered by a virus. The executable is forced to run.

If absolutely nothing happens, a self replicating virus does not exist. If anything within the environment changes (i.e. size of files, sudden attempts to write to other executables in the emulation box, etc.) it is determined that a virus does exist and is attempting to self replicate itself.

The first step is to determine whether the IRQ table was modified. The second step is to determine if another program was written to. Many programs attach themselves to IRQs (i.e. network shell programs, mouse drivers, some

SOPHOS
EXHIBIT 1004 - PAGE 0333

print drivers, communication and fax drivers). However, none of these programs will try to write code to other executables. No legitimate program will attempt direct changes to the File Allocation Table (FAT) or other internal OS disk area. They typically pass their changes (or writes) through standard well behaved DOS interrupts (INTs) (i.e. INT 21). Or, for example, in the case of file repair programs (i.e. Norton Utilities) which do at times write directly to the FAT, they will also not grab IRQs. It is the combination of grabbing one or more IRQs and attempting changes to either the FAT or executables that allows virus activity to be detected.

In the architecture of the IBM PC, for example, IRQs are prioritized and have different dedicated purposes. IRQ 0 is the system clock, IRQ 1 is the keyboard, etc. Almost no program needs to grab IRQ 0 having the highest priority, however a virus must. A virus must grab the highest priority IRQ because if it had a lower IRQ, then a conventional anti-virus program can get in at a higher priority and make the virus more vulnerable to detection. Many viruses grab several IRQs, allowing a virus to be detected by its 'signature'. In addition, most programs except viruses return to DOS about 95% or more of the memory they used for execution upon exiting or receiving an unload instruction. Therefore the following activities, monitored in the virtual environment created in the emulation box, can be used to detect viruses: attachment to IRQs, which IRQs have been attached, whether multiple IRQs have been attached, changes to the FAT, changes to executables, changes to the environment, changes to memory and any Terminate and Stay Resident (TSR) activity after the unload command has been issued and the program should have terminated.

In addition a further series of checks can then be initiated: check the "hard drive" and look for additional sectors or blocks being marked "bad" which were good before or vice versa. Has the program attached itself to the internal clock and is it incrementing its own internal clock? Have any of the error-checking algorithm results changed?

SOPHOS
EXHIBIT 1004 - PAGE 0334

Upon detection of a virus by the analysis and detection means 50, response/alarm means 52 can execute any number of user definable optional commands such as messaging or beeping a system administrator, notifying the sender and receiver of the file or program, deleting the file, writing to a specially prepared floppy drive, calling a pager with a virus message or shutting down a network segment. A logic flow diagram showing the operating steps the trap device 10 performs is shown in Figures 6A to 6C.

A high level logic diagram of the software is shown in Figure 5. The input data stream is generated by communication links 24. Link adapters 20 convert the data input stream from a hardware and software protocol specific to the particular communication link (i.e. X.25, Novell IPX/SPX, Microsoft NetBEUI, etc.) to a common protocol understandable by the CPU 12. After protocol conversion, the data packets are disassembled into a data stream having a common data format the CPU 12 is able to understand. The data is then processed and analyzed for the presence of virus activity. Following processing, data packets are re-assembled and converted to its original hardware and software protocol by the I/O Interface 18 before being output to the protected computer system 28.

The trap device 10 passes data directly through to the host system in addition to simultaneously processing it. This is to reduce the processing delays associated with sending large data files to the host system and having the trap device 10 process this data before the host receives it. The entire contents of a large file except for the final write command or the file close command is transmitted to the host. If no virus is detected, the write or close command is issued. If a virus is detected, the write or close is never issued and the response/alarm means 52 takes appropriate action.

It is clear that the above description of the preferred embodiment in no way limits the scope of the present invention which is defined by the following claims.

SOPHOS
EXHIBIT 1004 - PAGE 0335

What is claimed is:

1. A computer virus trapping device comprising:

link adapter means connected to a source of data input for converting external protocols into a data format understood by said trapping device;

emulation means connected to said link adapter means for accepting said data stream from said link adapter means; said emulation means providing an environment isolated from a protected computer system that simulates the architecture of said protected computer system whereby a computer virus is coaxed into performing its intended activity; and

detection means for monitoring said emulation means and determining when said computer virus either has performed or is performing its said intended activity.

2. The device of claim 1, whereby said emulation means comprises processing means suitably programmed to create a virtual world for said computer virus that simulates said protected computer system.

3. The device of claim 2, whereby said processing means comprises a microcomputer circuit, temporary and permanent data storage and an I/O interface.

4. A computer virus trapping device comprising:

link adapter means connected to a source of data input for converting external protocols into a data format understood by said trapping device;

emulation means connected to said link adapter means for accepting said data stream from said link adapter means; said emulation means providing an environment isolated from a protected computer system that simulates the architecture of said protected computer system whereby a computer virus is coaxed into performing its

SOPHOS
EXHIBIT 1004 - PAGE 0336

intended activity;

detection means for monitoring said emulation means and determining when said computer virus either has performed or is performing its said intended activity; and

response means responsive to said detection means to take action according to preset user instructions upon said detection means determining said computer virus exists.

5. A computer virus trapping device comprising:

link adapter means connected to a source of data input for bidirectionally converting external protocols into a converted data format understood by said trapping device;

emulation means connected to said link adapter means for accepting said data stream from said link adapter means; said emulation means providing an environment isolated from a protected computer system and simulating the architecture of said protected computer system so as to coax a computer virus into performing its intended activity;

detection means for monitoring said emulation means and determining when said computer virus either has performed or is performing its said intended activity;

response means responsive to said detection means to take action according to preset user instructions upon said detection means determisaid computer virus exists; and

I/O buffer means for reassembling said converted data back into said external data stream protocol and delivering said data stream to said protected computer system.

6. The device of claim 5, whereby said emulation means comprises microprocessor means programmed to simulate the environment of said protected computer system.

SOPHOS
EXHIBIT 1004 - PAGE 0337

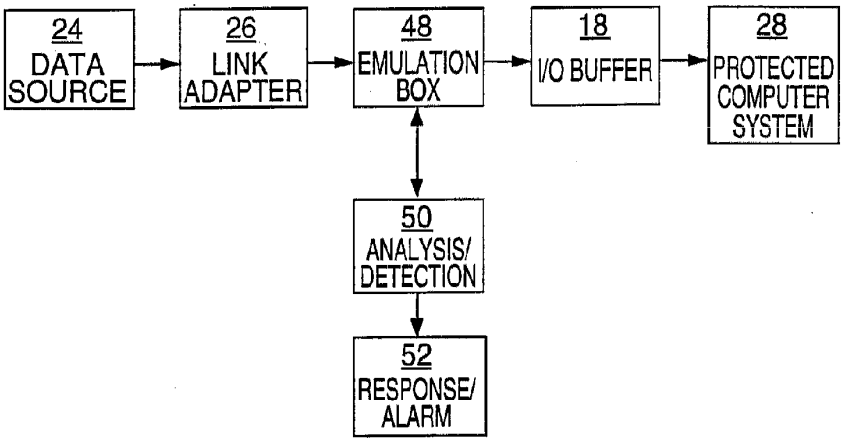


FIG. 1

DEF-FIN00007717

SOPHOS
EXHIBIT 1004 - PAGE 0338

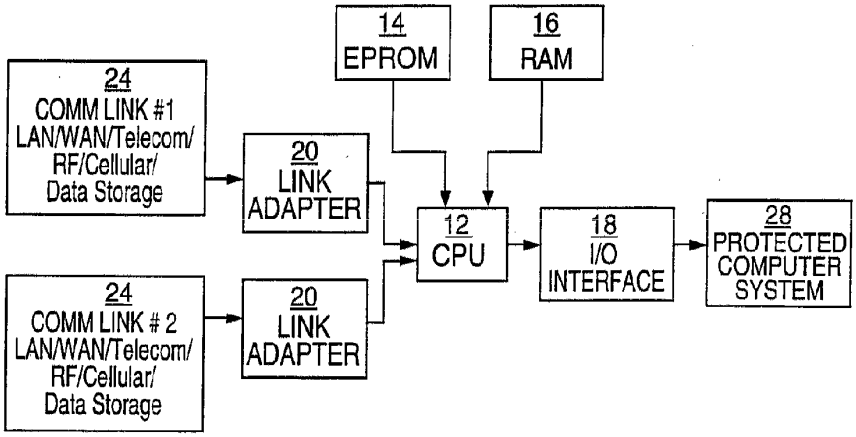


FIG. 2

DEF-FIN00007718

SOPHOS
EXHIBIT 1004 - PAGE 0339

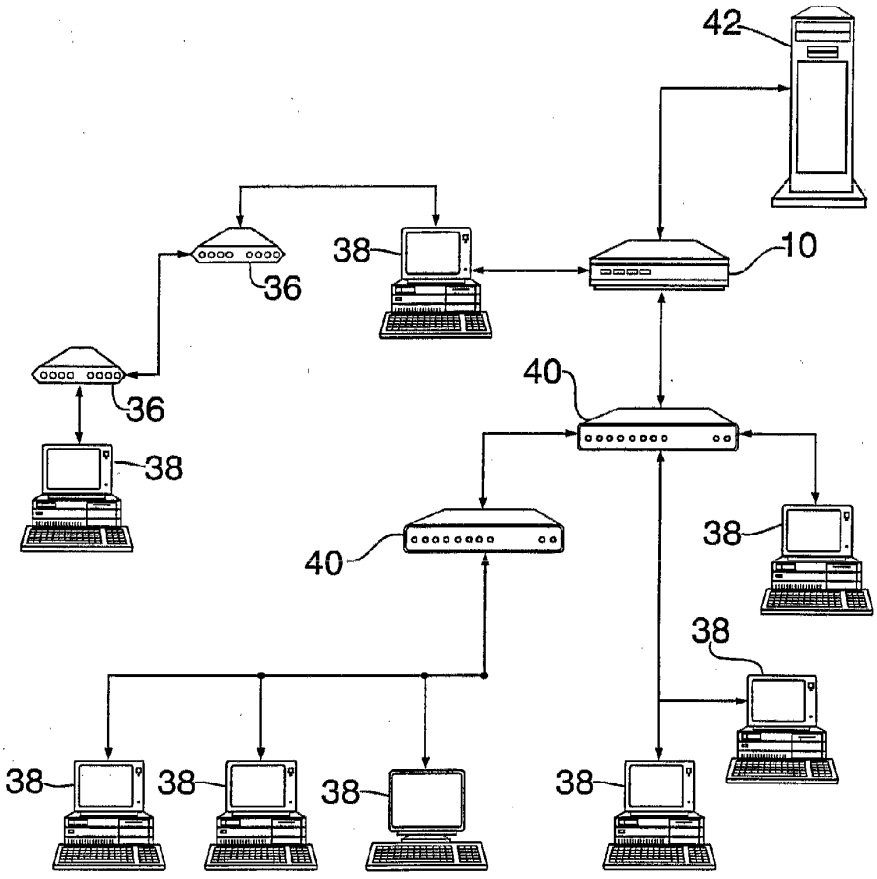


FIG. 3

DEF-FIN00007719

SOPHOS
EXHIBIT 1004 - PAGE 0340

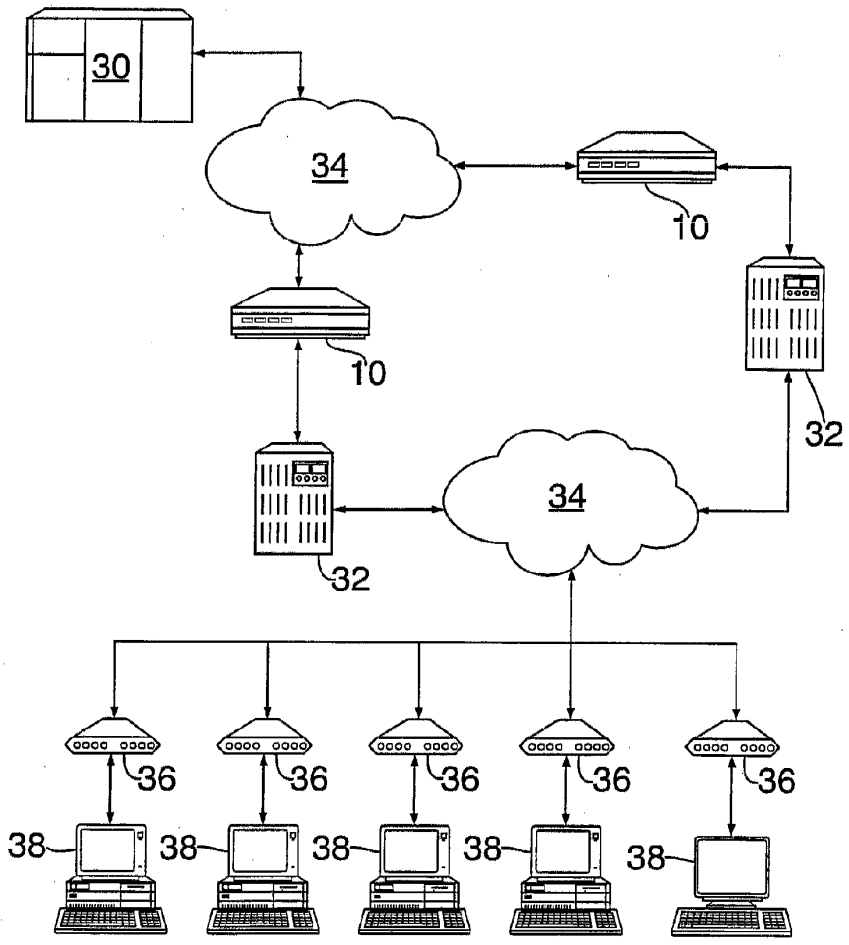


FIG. 4

DEF-FIN00007720

SOPHOS
EXHIBIT 1004 - PAGE 0341

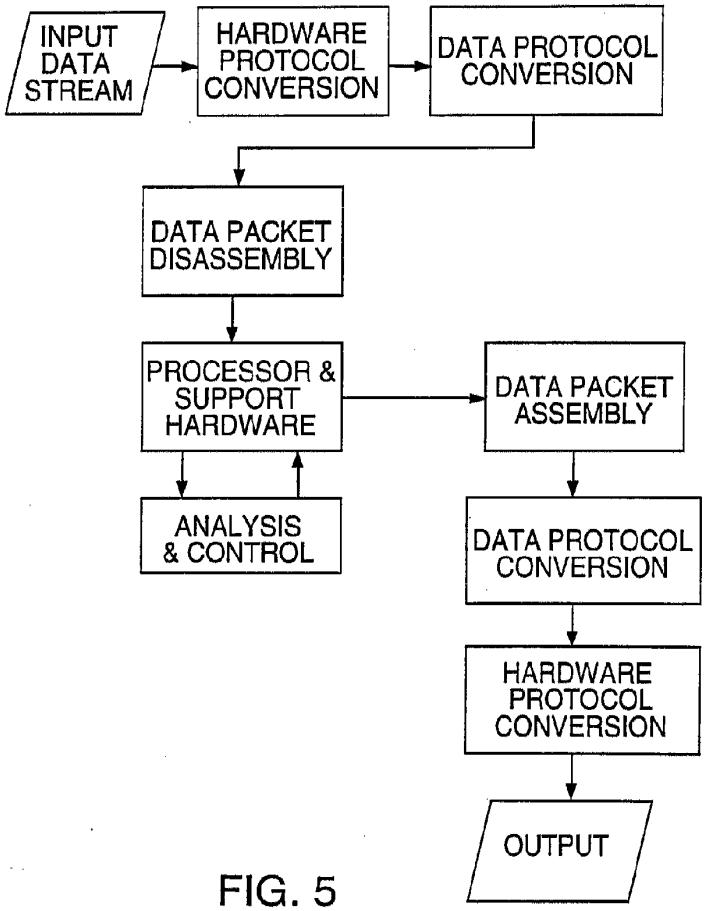


FIG. 5

SOPHOS
EXHIBIT 1004 - PAGE 0342

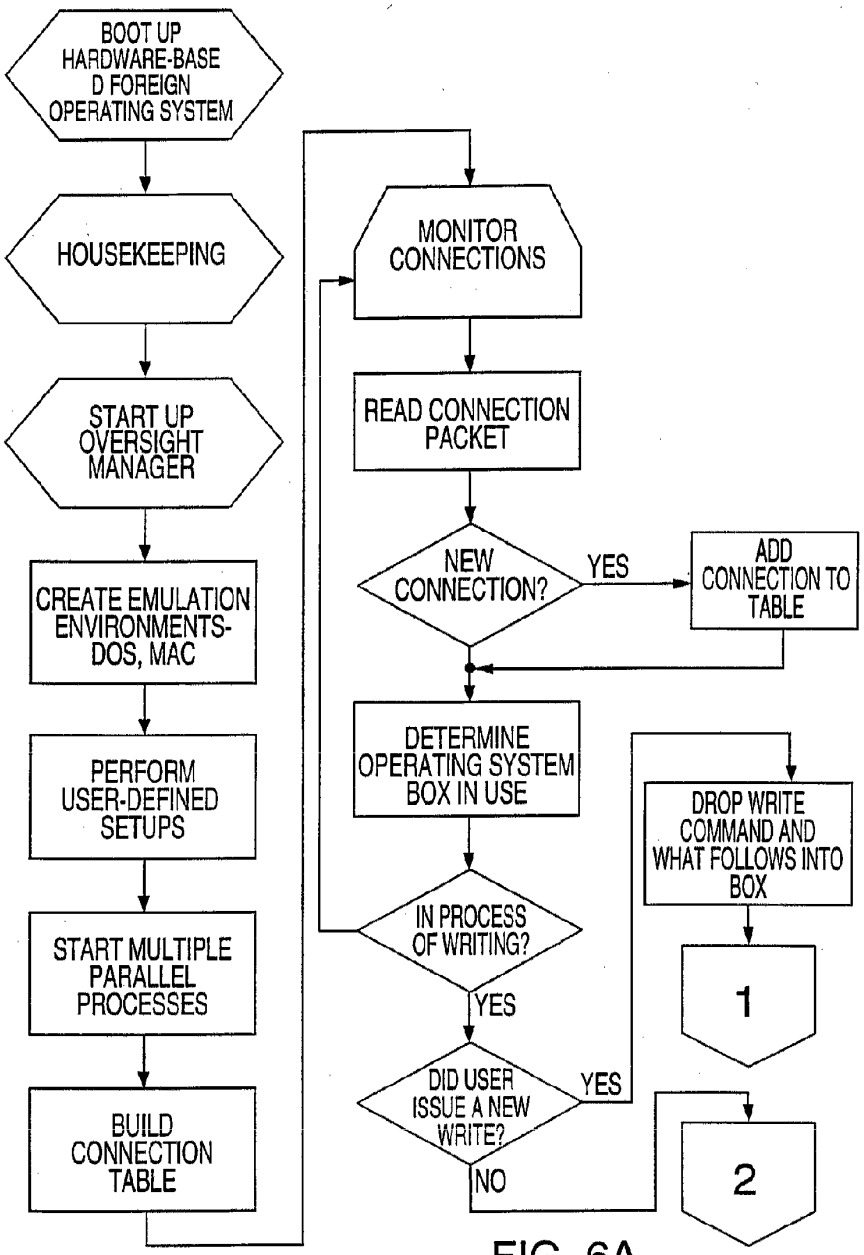


FIG. 6A

DEF-FIN00007722

SOPHOS
EXHIBIT 1004 - PAGE 0343

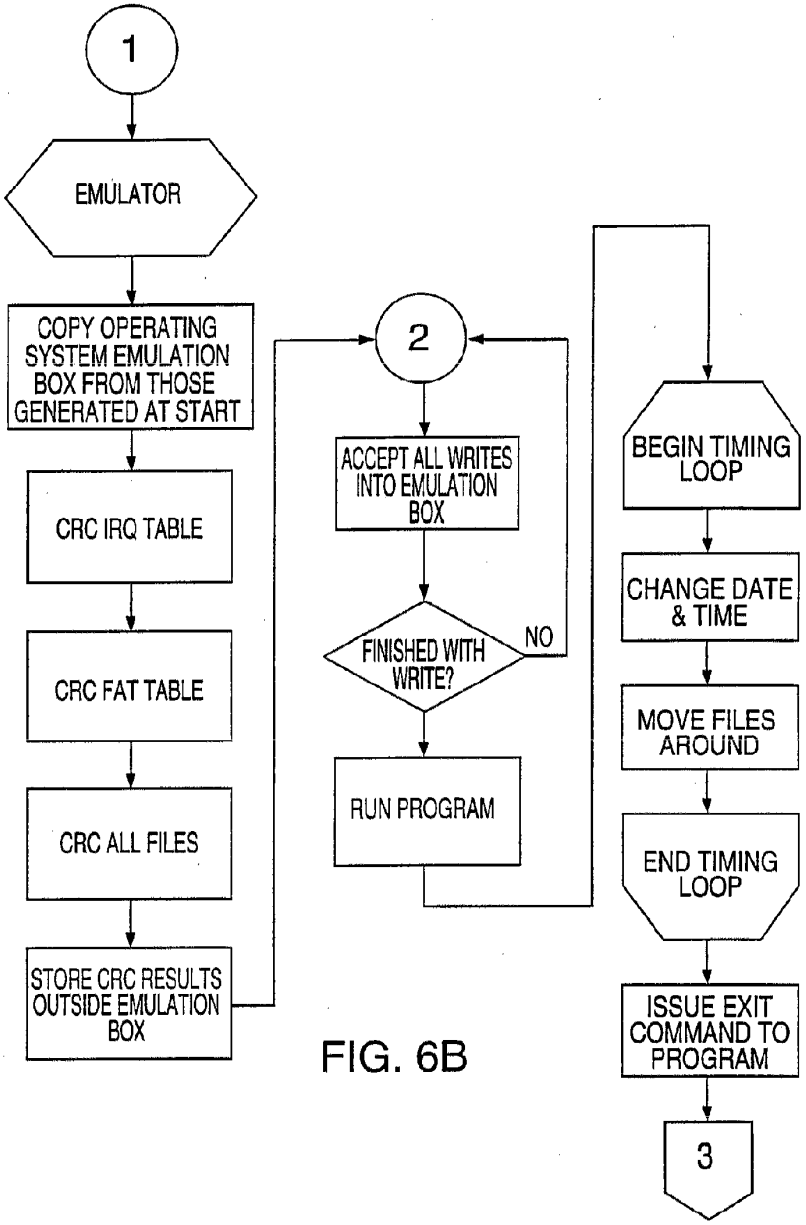


FIG. 6B

DEF-FIN00007723

SOPHOS
EXHIBIT 1004 - PAGE 0344

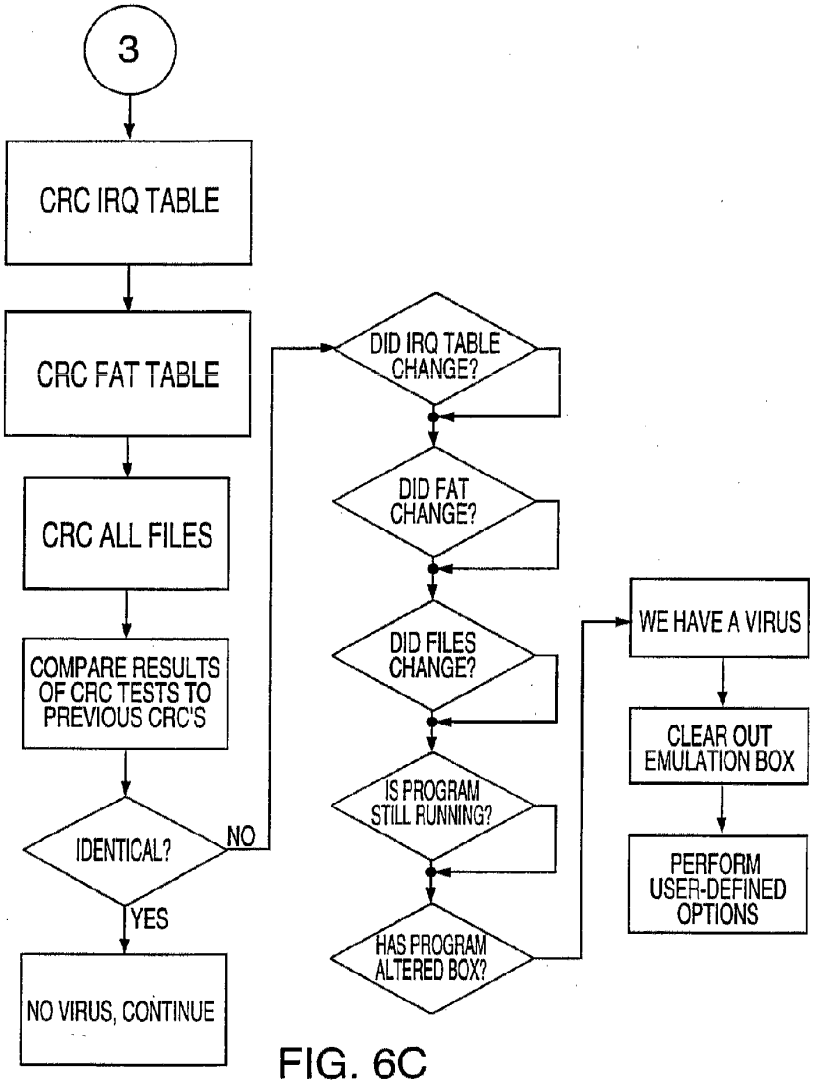


FIG. 6C

DEF-FIN00007724

SOPHOS
EXHIBIT 1004 - PAGE 0345

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/06659

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 11/00, 17/00
US CL : 395/500
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 395/500, 575; 371/16.2, 23

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, DIALOG,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	US, A, 5,398,196 (CHAMBERS) 14 March 1995, col. 3, lines 38-63, col. 4, lines 1-14, 58-et seq. and the claims.	1-6
A, E	US, A, 5,440,723(ARNOLD ET AL) 08 August 1995, see the enire document.	1-6
A	US, A, 5,274,815 (TRISSEL ET AL) 28 December 1993, see the entire document.	1-6
A,P	US, A, 5,359,659 (ROSENTHAL) 25 October 1994, see the entire document.	1-6

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 08 AUGUST 1995	Date of mailing of the international search report 13 SEP 1995
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer AYNI MOHAMED B. Mohamed for Telephone No. (703) 305-9694

Form PCT/ISA/210 (second sheet)(July 1992)*

DEF-FIN00007725

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 11/00 — A1

(11) International Publication Number: **WO 95/27249**

(43) International Publication Date: 12 October 1995 (12.10.95)

(21) International Application Number: PCT/US95/04109

(22) International Filing Date: 3 April 1995 (03.04.95)

(30) Priority Data:
08/223,221 5 April 1994 (05.04.94) US

(71) Applicant: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventor: TOUBOUL, Shlomo; 42495 Kefar Haim (IL).

(74) Agents: SALTER, James, H. et al.; Blakely, Sokoloff, Taylor & Zafman, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025-1026 (US).

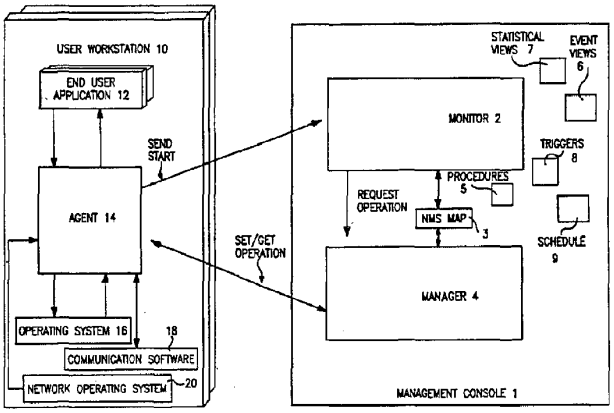
(81) Designated States: AM, AT, AT (Utility model), AU, BB, BG, BR, BY, CA, CH, CN, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), TJ, TM, TT, UA, UG, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND APPARTUS FOR MONITORING AND CONTROLLING PROGRAMS IN A NETWORK



(57) Abstract

A system for monitoring and controlling at least one program capable of being executed on any one of at least two workstations in a network. The network includes at least one agent module (14) resident on each of the at least two workstations (10) and a management console (1) connected to each of the at least two workstations (10). The system includes modules for identifying an event occuring with respect to a program executing on one of the at least two workstations (10), modules for sending an alert to the management console (1) which identifies the event, memory for storing a plurality of triggers (8), each of the triggers (8) adapted to cause an action to be taken within the network, memory for storing at least one procedure (5) comprising at least one of the plurality of triggers (8), and modules for sending at least one of the procedures (5) from the management console (1) to the agent module (14) resident on the one of the at least two workstations (10) in response to receipt of the alert. A method is also provided for monitoring and controlling programs capable of being executed on any of at least two workstations (10) in a network.

SOPHOS
EXHIBIT 1004 - PAGE 0347

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K

A2

(11) International Publication Number: **WO 98/21683**

(43) International Publication Date: 22 May 1998 (22.05.98)

(21) International Application Number: PCT/IB97/01626

(22) International Filing Date: 6 November 1997 (06.11.97)

(30) Priority Data:

60/030,639	8 November 1996 (08.11.96)	US
Not furnished	6 November 1997 (06.11.97)	US

(71) Applicant: FINJAN SOFTWARE, LTD. [IL/IL]; 42945 Kefar-Haim (IL).

(72) Inventor: TOUBOUL, Shlomo; 42945 Kefar-Haim (IL).

(81) Designated States: CA, IL, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

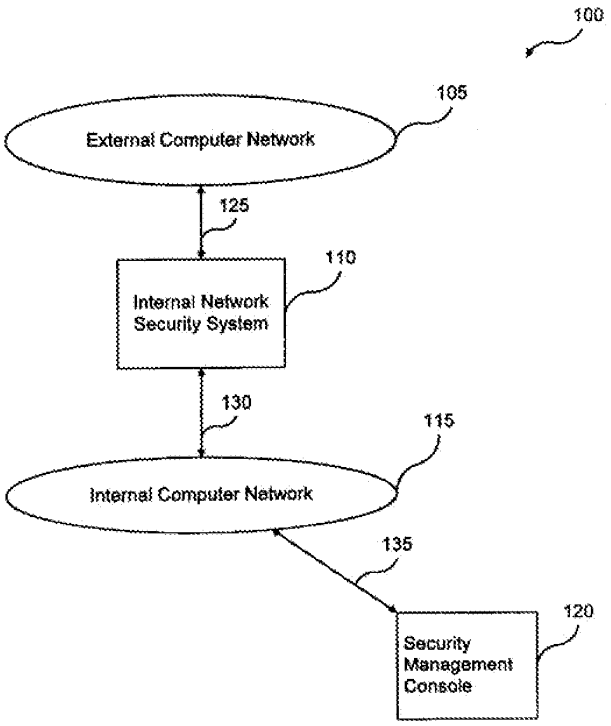
Published

Without international search report and to be republished upon receipt of that report.

(54) Title: SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

(57) Abstract

A system protects a computer from suspicious Downloadables. The system comprises a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to the Downloadable to determine if the security policy has been violated. The Downloadable may include a Java™ applet, an ActiveX™ control, a JavaScript™ script, or a Visual Basic script. The security policy may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, or a specific security policy to be applied based on the client or the group to which the client belongs. The system uses an ID generator to compute a Downloadables ID identifying the Downloadable, preferably, by fetching all components of the Downloadable and performing a hashing function on the Downloadable including the fetched components. Further, the security policy may indicate several tests to perform, including (1) a comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables to be blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile data against access control lists; (4) a comparison of a certificate embodied in the Downloadable against trusted certificates; and (5) a comparison of the URL from which the Downloadable originated against trusted and untrusted URLs. Based on these tests, a logical engine can determine whether to allow or block the Downloadable.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SOPHOS
EXHIBIT 1004 - PAGE 0349

SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to computer networks, and more particularly provides a system and method for protecting a computer and a network from hostile Downloadables.

2. Description of the Background Art

The Internet is currently a collection of over 100,000 individual computer networks owned by governments, universities, nonprofit groups and companies, and is expanding at an accelerating rate. Because the Internet is public, the Internet has become a major source of many system damaging and system fatal application programs, commonly referred to as "viruses."

Accordingly, programmers continue to design computer and computer network security systems for blocking these viruses from attacking both individual and network computers. On the most part, these security systems have been relatively successful. However, these security systems are not configured to recognize computer viruses which have been attached to or configured as Downloadable application programs, commonly referred to as "Downloadables." A Downloadable is an executable application program, which is downloaded from a source computer and run on the destination computer. Downloadable is typically requested by an ongoing process such as by an Internet browser or web engine. Examples of Downloadables include Java™ applets designed for use in the Java™ distributing environment developed by Sun Microsystems, Inc., JavaScript scripts also

SOPHOS
EXHIBIT 1004 - PAGE 0350

developed by Sun Microsystems, Inc., ActiveX™ controls designed for use in the ActiveX™ distributing environment developed by the Microsoft Corporation, and Visual Basic also developed by the Microsoft Corporation. Therefore, a system and method are needed to protect a network from hostile Downloadables.

5

SUMMARY OF THE INVENTION

The present invention provides a system for protecting a network from suspicious Downloadables. The system comprises a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to 10 the Downloadable to determine if the security policy has been violated. The Downloadable may include a Java™ applet, an ActiveX™ control, a JavaScript™ script, or a Visual Basic script. The security policy may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, a specific security policy to be applied based on the client or the group to which the client belongs, or a specific policy to be applied 15 based on the client/group and on the particular Downloadable received. The system uses an ID generator to compute a Downloadable ID identifying the Downloadable, preferably, by fetching all components of the Downloadable and performing a hashing function on the Downloadable including the fetched components.

Further, the security policy may indicate several tests to perform, including (1) a 20 comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables to be blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile data against access control lists; (4) a comparison of a certificate embodied in the Downloadable against trusted certificates; and (5) a comparison of the URL from which the Downloadable originated against trusted and untrusted URLs.

SOPHOS
EXHIBIT 1004 - PAGE 0351

Based on these tests, a logical engine can determine whether to allow or block the Downloadable.

The present invention further provides a method for protecting a computer from suspicious Downloadables. The method comprises the steps of receiving a Downloadable, comparing the Downloadable against a security policy to determine if the security policy has been violated, and discarding the Downloadable if the security policy has been violated.

It will be appreciated that the system and method of the present invention may provide computer protection from known hostile Downloadables. The system and method of the present invention may identify Downloadables that perform operations deemed suspicious. The system and method of the present invention may examine the Downloadable code to determine whether the code contains any suspicious operations, and thus may allow or block the Downloadable accordingly.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating a network system, in accordance with the present invention;

FIG. 2 is a block diagram illustrating details of the internal network security system of FIG. 1;

FIG. 3 is a block diagram illustrating details of the security program and the security database of FIG. 2;

FIG. 4 is a block diagram illustrating details of the security policies of FIG. 3;

FIG. 5 is a block diagram illustrating details of the security management console of FIG. 1;

SOPHOS
EXHIBIT 1004 - PAGE 0352

FIG. 6A is a flowchart illustrating a method of examining for suspicious Downloadables, in accordance with the present invention;

FIG. 6B is a flowchart illustrating details of the step for finding the appropriate security policy of FIG. 6A;

FIG. 6C is a flowchart illustrating a method for determining whether an incoming Downloadable is to be deemed suspicious;

FIG. 7 is a flowchart illustrating details of the FIG. 6 step of decomposing a Downloadable; and

FIG. 8 is a flowchart illustrating a method 800 for generating a Downloadable ID for identifying a Downloadable.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 is a block diagram illustrating a network system 100, in accordance with the present invention. The network system 100 includes an external computer network 105, such as the Wide Area Network (WAN) commonly referred to as the Internet, coupled via a communications channel 125 to an internal network security system 110. The network system 100 further includes an internal computer network 115, such as a corporate Local Area Network (LAN), coupled via a communications channel 130 to the internal network computer system 110 and coupled via a communications channel 135 to a security management console 120.

The internal network security system 110 examines Downloadables received from external computer network 105, and prevents Downloadables deemed suspicious from reaching the internal computer network 115. It will be further appreciated that a Downloadable is deemed suspicious if it performs or may perform any undesirable operation.

SOPHOS
EXHIBIT 1004 - PAGE 0353

or if it threatens or may threaten the integrity of an internal computer network 115 component. It is to be understood that the term "suspicious" includes hostile, potentially hostile, undesirable, potentially undesirable, etc. Security management console 120 enables viewing, modification and configuration of the internal network security system 110.

FIG. 2 is a block diagram illustrating details of the internal network security system 110, which includes a Central Processing Unit (CPU) 205, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a signal bus 220. The internal network security system 110 further includes an external communications interface 210 coupled between the communications channel 125 and the signal bus 220 for receiving Downloadables from external computer network 105, and an internal communications interface 225 coupled between the signal bus 220 and the communications channel 130 for forwarding Downloadables not deemed suspicious to the internal computer network 115. The external communications interface 210 and the internal communications interface 225 may be functional components of an integral communications interface (not shown) for both receiving Downloadables from the external computer network 105 and forwarding Downloadables to the internal computer network 115.

Internal network security system 110 further includes Input/Output (I/O) interfaces 215 (such as a keyboard, mouse and Cathode Ray Tube (CRT) display), a data storage device 230 such as a magnetic disk, and a Random-Access Memory (RAM) 235, each coupled to the signal bus 220. The data storage device 230 stores a security database 240, which includes security information for determining whether a received Downloadable is to be deemed suspicious. The data storage device 230 further stores a users list 260 identifying the users within the internal computer network 115 who may receive Downloadables, and an

SOPHOS
EXHIBIT 1004 - PAGE 0354

event log 245 which includes determination results for each Downloadable examined and runtime indications of the internal network security system 110. An operating system 250 controls processing by CPU 205, and is typically stored in data storage device 230 and loaded into RAM 235 (as illustrated) for execution. A security program 255 controls examination of incoming Downloadables, and also may be stored in data storage device 230 and loaded into RAM 235 (as illustrated) for execution by CPU 205.

FIG. 3 is a block diagram illustrating details of the security program 255 and the security database 240. The security program 255 includes an ID generator 315, a policy finder 317 coupled to the ID generator 315, and a first comparator 320 coupled to the policy finder 317. The first comparator 320 is coupled to a logical engine 333 via four separate paths, namely, via Path 1, via Path 2, via Path 3 and via Path 4. Path 1 includes a direct connection from the first comparator 320 to the logical engine 333. Path 2 includes a code scanner coupled to the first comparator 320, and an Access Control List (ACL) comparator 330 coupling the code scanner 325 to the logical engine 333. Path 3 includes a certificate scanner 340 coupled to the first comparator 320, and a certificate comparator 345 coupling the certificate scanner 340 to the logical engine 333. Path 4 includes a Uniform Resource Locator (URL) comparator 350 coupling the first comparator 320 to the logical engine 3330. A record-keeping engine 335 is coupled between the logical engine 333 and the event log 245.

The security program 255 operates in conjunction with the security database 240, which includes security policies 305, known Downloadables 307, known Certificates 309 and Downloadable Security Profile (DSP) data 310 corresponding to the known Downloadables 307. Security policies 305 includes policies specific to particular users 260

SOPHOS
EXHIBIT 1004 - PAGE 0355

and default (or generic) policies for determining whether to allow or block an incoming Downloadable. These security policies 305 may identify specific Downloadables to block, specific Downloadables to allow, or necessary criteria for allowing an unknown Downloadable. Referring to FIG. 4, security policies 305 include policy selectors 405, access control lists 410, trusted certificate lists 415, URL rule bases 420, and lists 425 of Downloadables to allow or to block per administrative override.

Known Downloadables 307 include lists of Downloadables which Original Equipment Manufacturers (OEMs) know to be hostile, of Downloadables which OEMs know to be non-hostile, and of Downloadables previously received by this security program 255. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by each known Downloadable 307, and may also include the respective arguments of these operations. An identified argument of an operation is referred to as "resolved." An unidentified argument is referred to as "unresolved." DSP data 310 is described below with reference to the code scanner 325.

The ID generator 315 receives a Downloadable (including the URL from which it came and the userID of the intended recipient) from the external computer network 105 via the external communications interface 210, and generates a Downloadable ID for identifying each Downloadable. The Downloadable ID preferably includes a digital hash of the complete Downloadable code. The ID generator 315 preferably prefetches all components embodied in or identified by the code for Downloadable ID generation. For example, the ID generator 315 may prefetch all classes embodied in or identified by the Java™ applet bytecode to generate the Downloadable ID. Similarly, the ID generator 315 may retrieve all components listed in the .INF file for an ActiveX™ control to compute a Downloadable ID. Accordingly, the Downloadable ID for the Downloadable will be the same each time the ID

SOPHOS
EXHIBIT 1004 - PAGE 0356

generator 315 receives the same Downloadable. The ID generator 315 adds the generated Downloadable ID to the list of known Downloadables 307 (if it is not already listed). The ID generator 315 then forwards the Downloadable and Downloadable ID to the policy finder 317.

The policy finder 317 uses the userID of the intended user and the Downloadable ID to select the specific security policy 305 that shall be applied on the received Downloadable. If there is a specific policy 305 that was defined for the user (or for one of its super groups) and the Downloadable, then the policy is selected. Otherwise the generic policy 305 that was defined for the user (or for one of its super groups) is selected. The policy finder 317 then sends the policy to the first comparator 320.

The first comparator 320 receives the Downloadable, the Downloadable ID and the security policy 305 from the policy finder 317. The first comparator 320 examines the security policy 305 to determine which steps are needed for allowing the Downloadable. For example, the security policy 305 may indicate that, in order to allow this Downloadable, it must pass all four paths, Path 1, Path 2, Path 3 and Path 4. Alternatively, the security policy 305 may indicate that to allow the Downloadable, the it must pass only one of the paths. The first comparator 320 responds by forwarding the proper information to the paths identified by the security policy 305.

Path 1

In path 1, the first comparator 320 checks the policy selector 405 of the security policy 305 that was received from the policy finder 317. If the policy selector 405 is either "Allowed" or "Blocked," then the first comparator 320 forwards this result directly to the logical engine 333. Otherwise, the first comparator 320 invokes the comparisons in path2

SOPHOS
EXHIBIT 1004 - PAGE 0357

and/or path 3 and/or path 4 based on the contents of policy selector 405. It will be appreciated that the first comparator 320 itself compares the Downloadable ID against the lists of Downloadables to allow or block per administrative override 425. That is, the system security administrator can define specific Downloadables as "Allowed" or "Blocked."

Alternatively, the logical engine 333 may receive the results of each of the paths and based on the policy selector 405 may institute the final determination whether to allow or block the Downloadable. The first comparator 320 informs the logical engine 333 of the results of its comparison.

Path 2

In path 2, the first comparator 320 delivers the Downloadable, the Downloadable ID and the security policy 305 to the code scanner 325. If the DSP data 310 of the received Downloadable is known, the code scanner 325 retrieves and forwards the information to the ACL comparator 330. Otherwise, the code scanner 325 resolves the DSP data 310. That is, the code scanner 325 uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data 310. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable 307, and may also include the respective arguments of these operations. For example, DSP data 310 may include a READ from a specific file, a SEND to an unresolved host, etc. The code scanner 325 may generate the DSP data 310 as a list of all operations in the Downloadable code which could ever be deemed potentially hostile and a list of all files to be accessed by the Downloadable code. It will be appreciated that the code scanner 325 may search the code for any pattern, which is undesirable or suggests that the code was written by a hacker.

SOPHOS
EXHIBIT 1004 - PAGE 0358

An Example List of Operations Deemed Potentially Hostile

- File operations: READ a file, WRITE a file;
- Network operations: LISTEN on a socket, CONNECT to a socket, SEND data, RECEIVE data, VIEW INTRANET;
- Registry operations: READ a registry item, WRITE a registry item;
- Operating system operations: EXIT WINDOWS, EXIT BROWSER, START PROCESS/THREAD, KILL PROCESS/THREAD, CHANGE PROCESS/THREAD PRIORITY, DYNAMICALLY LOAD A CLASS/LIBRARY, etc.; and
- Resource usage thresholds: memory, CPU, graphics, etc.

In the preferred embodiment, the code scanner 325 performs a full-content inspection. However, for improved speed but reduced security, the code scanner 325 may examine only a portion of the Downloadable such as the Downloadable header. The code scanner 325 then stores the DSP data into DSP data 310 (corresponding to its Downloadable ID), and sends the Downloadable, the DSP data to the ACL comparator 330 for comparison with the security policy 305.

The ACL comparator 330 receives the Downloadable, the corresponding DSP data and the security policy 305 from the code scanner 325, and compares the DSP data against the security policy 305. That is, the ACL comparator 330 compares the DSP data of the received Downloadable against the access control lists 410 in the received security policy 305. The access control list 410 contains criteria indicating whether to pass or fail the Downloadable. For example, an access control list may indicate that the Downloadable fails

SOPHOS
EXHIBIT 1004 - PAGE 0359

if the DSP data includes a WRITE command to a system file. The ACL comparator 330 sends its results to the logical engine 333.

Path 3:

In path 3, the certificate scanner 340 determines whether the received Downloadable was signed by a certificate authority, such as VeriSign, Inc., and scans for a certificate embodied in the Downloadable. The certificate scanner 340 forwards the found certificate to the certificate comparator 345. The certificate comparator 345 retrieves known certificates 309 that were deemed trustworthy by the security administrator and compares the found certificate with the known certificates 309 to determine whether the Downloadable was signed by a trusted certificate. The certificate comparator 345 sends the results to the logical engine 333.

Path 4:

In path 4, the URL comparator 350 examines the URL identifying the source of the Downloadable against URLs stored in the URL rule base 420 to determine whether the Downloadable comes from a trusted source. Based on the security policy 305, the URL comparator 350 may deem the Downloadable suspicious if the Downloadable comes from an untrustworthy source or if the Downloadable did not come from a trusted source. For example, if the Downloadable comes from a known hacker, then the Downloadable may be deemed suspicious and presumed hostile. The URL comparator 350 sends its results to the logical engine 333.

SOPHOS
EXHIBIT 1004 - PAGE 0360

The logical engine 333 examines the results of each of the paths and the policy selector 405 in the security policy 305 to determine whether to allow or block the Downloadable. The policy selector 405 includes a logical expression of the results received from each of the paths. For example, the logical engine 333 may block a Downloadable if it fails any one of the paths, i.e., if the Downloadable is known hostile (Path 1), if the Downloadable may request suspicious operations (Path 2), if the Downloadable was not signed by a trusted certificate authority (Path 3), or if the Downloadable did came from an untrustworthy source (Path 4). The logical engine 333 may apply other logical expressions according to the policy selector 405 embodied in the security policy 305. If the policy selector 405 indicates that the Downloadable may pass, then the logical engine 333 passes the Downloadable to its intended recipient. Otherwise, if the policy selector 405 indicates that the Downloadable should be blocked, then the logical engine 333 forwards a non-hostile Downloadable to the intended recipient to inform the user that internal network security system 110 discarded the original Downloadable. Further, the logical engine 333 forwards a status report to the record-keeping engine 335, which stores the reports in event log 245 in the data storage device 230 for subsequent review, for example, by the MIS director.

FIG. 5 is a block diagram illustrating details of the security management console 120, which includes a security policy editor 505 coupled to the communications channel 135, an event log analysis engine 510 coupled between communications channel 135 and a user notification engine 515, and a Downloadable database review engine 520 coupled to the communications channel 135. The security management console 120 further includes computer components similar to the computer components illustrated in FIG. 2.

SOPHOS
EXHIBIT 1004 - PAGE 0361

The security policy editor 505 uses an I/O interface similar to I/O interface 215 for enabling authorized user modification of the security policies 305. That is, the security policy editor 505 enables the authorized user to modify specific security policies 305 corresponding to the users 260, the default or generic security policy 305, the Downloadables to block per administrative override, the Downloadables to allow per administrative override, the trusted certificate lists 415, the policy selectors 405, the access control lists 410, the URLs in the URL rule bases 420, etc. For example, if the authorized user learns of a new hostile Downloadable, then the user can add the Downloadable to the Downloadables to block per system override.

The event log analysis engine 510 examines the status reports contained in the event log 245 stored in the data storage device 230. The event log analysis engine 510 determines whether notification of the user (e.g., the security system manager or MIS director) is warranted. For example, the event log analysis engine 510 may warrant user notification whenever ten (10) suspicious Downloadables have been discarded by internal network security system 110 within a thirty (30) minute period, thereby flagging a potential imminent security threat. Accordingly, the event log analysis engine 510 instructs the user notification engine 515 to inform the user. The user notification engine 515 may send an e-mail via internal communications interface 220 or via external communications interface 210 to the user, or may display a message on the user's display device (not shown).

FIG. 6A is a flowchart illustrating a method 600 for protecting an internal computer network 115 from suspicious Downloadables. Method 600 begins with the ID generator 315 in step 602 receiving a Downloadable. The ID generator 315 in step 604 generates a Downloadable ID identifying the received Downloadable, preferably, by generating a digital

SOPHOS
EXHIBIT 1004 - PAGE 0362

hash of the Downloadable code (including prefetched components). The policy finder 317 in step 606 finds the appropriate security policy 305 corresponding to the userID specifying intended recipient (or the group to which the intended recipient belongs) and the Downloadable. The selected security policy 305 may be the default security policy 305. Step 606 is described in greater detail below with reference to FIG. 6B.

The first comparator 320 in step 608 examines the lists of Downloadables to allow or to block per administrative override 425 against the Downloadable ID of the incoming Downloadable to determine whether to allow the Downloadable automatically. If so, then in step 612 the first comparator 320 sends the results to the logical engine 333. If not, then the method 600 proceeds to step 610. In step 610, the first comparator 620 examines the lists of Downloadables to block per administrative override 425 against the Downloadable ID of the incoming Downloadable for determining whether to block the Downloadable automatically. If so, then the first comparator 420 in step 612 sends the results to the logical engine 333. Otherwise, method 600 proceeds to step 614.

In step 614, the first comparator 320 determines whether the security policy 305 indicates that the Downloadable should be tested according to Path 4. If not, then method 600 jumps to step 618. If so, then the URL comparator 350 in step 616 compares the URL embodied in the incoming Downloadable against the URLs of the URL rules bases 420, and then method 600 proceeds to step 618.

In step 618, the first comparator 320 determines whether the security policy 305 indicates that the Downloadable should be tested according to Path 2. If not, then method 600 jumps to step 620. Otherwise, the code scanner 235 in step 626 examines the DSP data 310 based on the Downloadable ID of the incoming Downloadable to determine whether the Downloadable has been previously decomposed. If so, then method 600 jumps to step 630.

SOPHOS
EXHIBIT 1004 - PAGE 0363

Otherwise, the code scanner 325 in step 628 decomposes the Downloadable into DSP data. Downloadable decomposition is described in greater detail with reference to FIG. 7. In step 630, the ACL comparator 330 compares the DSP data of the incoming Downloadable against the access control lists 410 (which include the criteria necessary for the Downloadable to fail or pass the test).

In step 620, the first comparator 320 determines whether the security policy 305 indicates that the Downloadable should be tested according to Path 3. If not, then method 600 returns to step 612 to send the results of each of the test performed to the logical engine 333. Otherwise, the certificate scanner 622 in step 622 scans the Downloadable for an embodied certificate. The certificate comparator 345 in step 624 retrieves trusted certificates from the trusted certificate lists (TCL) 415 and compares the embodied certificate with the trusted certificates to determine whether the Downloadable has been signed by a trusted source. Method 600 then proceeds to step 612 by the certificate scanner 345 sending the results of each of the paths taken to the logical engine 333. The operations of the logical engine 333 are described in greater detail below with reference to FIG. 6C. Method 600 then ends.

One skilled in the art will recognize that the tests may be performed in a different order, and that each of the tests need not be performed. Further, one skilled in the art will recognize that, although path 1 is described in FIG. 6A as an automatic allowance or blocking, the results of Path 1 may be another predicate to be applied by the logical engine 333. Further, although the tests are shown serially in FIG. 6A, the tests may be performed in parallel as illustrated in FIG. 3.

SOPHOS
EXHIBIT 1004 - PAGE 0364

FIG. 6B is a flowchart illustrating details of step 606 of FIG. 6A (referred to herein as method 606). Method 606 begins with the policy finder 317 in step 650 determining whether security policies 305 include a specific security policy corresponding to the userID and the Downloadable. If so, then the policy finder 317 in step 654 fetches the corresponding specific policy 305. If not, then the policy finder 317 in step 652 fetches the default or generic security policy 305 corresponding to the userID. Method 606 then ends.

FIG. 6C is a flowchart illustrating details of a method 655 for determining whether to allow or to block the incoming Downloadable. Method 655 begins with the logical engine 333 in step 660 receiving the results from the first comparator 320, from the ACL comparator 330, from the certificate comparator 345 and from the URL comparator 350. The logical engine 333 in step 662 compares the results with the policy selector 405 embodied in the security policy 305, and in step 664 determines whether the policy selector 405 confirms the pass. For example, the policy selector 405 may indicate that the logical engine 333 pass the Downloadable if it passes one of the tests of Path 1, Path 2, Path 3 and Path 4. If the policy selector 405 indicates that the Downloadable should pass, then the logical engine 333 in step 666 passes the Downloadable to the intended recipient. In step 668, the logical engine 333 sends the results to the record-keeping engine 335, which in turn stores the results in the event log 245 for future review. Method 655 then ends. Otherwise, if the policy selector 405 in step 664 indicates that the Downloadable should not pass, then the logical engine 333 in step 670 stops the Downloadable and in step 672 sends a non-hostile substitute Downloadable to inform the user that the incoming Downloadable has been blocked. Method 655 then jumps to step 668.

SOPHOS
EXHIBIT 1004 - PAGE 0365

FIG. 7 is a flowchart illustrating details of step 628 of FIG. 6A (referred to herein as method 628) for decomposing a Downloadable into DSP data 310. Method 628 begins in step 705 with the code scanner 325 disassembling the machine code of the Downloadable. The code scanner 325 in step 710 resolves a respective command in the machine code, and in step 715 determines whether the resolved command is suspicious (e.g., whether the command is one of the operations identified in the list described above with reference to FIG. 3). If not, then the code scanner 325 in step 725 determines whether it has completed decomposition of the Downloadable, i.e., whether all operations in the Downloadable code have been resolved. If so, then method 628 ends. Otherwise, method 628 returns to step 710.

Otherwise, if the code scanner 325 in step 715determines that the resolved command is suspect, then the code scanner 325 in step 720 decodes and registers the suspicious command and its command parameters as DSP data 310. The code scanner 325 in step 720 registers the commands and command parameters into a format based on command class (e.g., file operations, network operations, registry operations, operating system operations, resource usage thresholds). Method 628 then jumps to step 725.

FIG. 8 is a flowchart illustrating a method 800 for generating a Downloadable ID for identifying a Downloadable. Method 800 begins with the ID generator 315 in step 810 receiving a Downloadable from the external computer network 105. The ID generator 315 in step 820 may fetch some or all components referenced in the Downloadable code, and in step 830 includes the fetched components in the Downloadable code. The ID generator 315 in step 840 performs a hashing function on at least a portion of the Downloadable code to generate a Downloadable ID. The ID generator 315 in step 850 stores the generated

SOPHOS
EXHIBIT 1004 - PAGE 0366

Downloadable ID in the security database 240 as a reference to the DSP data 310. Accordingly, the Downloadable ID will be the same for the identical Downloadable each time it is encountered.

The foregoing description of the preferred embodiments of the invention is by way of example only, and other variations of the above-described embodiments and methods are provided by the present invention. For example, although the invention has been described in a system for protecting an internal computer network, the invention can be embodied in a system for protecting an individual computer. Components of this invention may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. The embodiments described herein have been presented for purposes of illustration and are not intended to be exhaustive or limiting. Many variations and modifications are possible in light of the foregoing teaching. The system is limited only by the following claims.

SOPHOS
EXHIBIT 1004 - PAGE 0367

WHAT IS CLAIMED IS:

1. A computer-based method, comprising the steps of:

receiving a Downloadable;

comparing the Downloadable against a security policy to determine if the security policy has been violated; and

discarding the Downloadable if the security policy has been violated.

2. The method of claim 1, further comprising the steps of decomposing the Downloadable into Downloadable security profile data, and comparing the Downloadable security profile data against the security policy.

3. The method of claim 1, further comprising the steps of scanning for a certificate and comparing the certificate against a trusted certificate.

4. The method of claim 1, further comprising the step of comparing the URL from which the Downloadable originated against a known URL.

5. The method of claim 4, wherein the known URL is a trusted URL.

6. The method of claim 4, wherein the known URL is an untrusted URL.

7. The method of claim 1, wherein the Downloadable includes a Java™ applet.

SOPHOS
EXHIBIT 1004 - PAGE 0368

8. The method of claim 1, wherein the Downloadable includes an ActiveX™ control.

9. The method of claim 1, wherein the Downloadable includes a JavaScript™ script.

10. The method of claim 1, wherein the Downloadable includes a Visual Basic script.

11. The method of claim 1, wherein

the Downloadable is addressed to a client; and

the security policy includes a default security policy to be applied regardless of the client to whom the Downloadable is addressed.

12. The method of claim 1, wherein

the Downloadable is addressed to a client; and

the security policy includes a specific security policy to be applied if the Downloadable is addressed to the client.

13. The method of claim 1, wherein

the Downloadable is addressed to a client belonging to a group; and

the security policy includes a specific security policy to be applied if the client belongs to a particular group.

SOPHOS
EXHIBIT 1004 - PAGE 0369

14. The method of claim 1,

wherein the Downloadable is addressed to a client; and

further comprising, after discarding the Downloadable, the step of sending a substitute non-hostile Downloadable to the client for informing the client.

15. The method of claim 1, further comprising, after discarding the Downloadable, the step of recording the violation in an event log.

16. The method of claim 1, further comprising the step of computing a Downloadable ID to identify the Downloadable.

17. The method of claim 16, further comprising the steps of fetching components identified by the Downloadable and including the fetched components in the Downloadable.

18. The method of claim 17, further comprising the step of performing a hashing function on the Downloadable.

19. The method of claim 17, further comprising the step of fetching all components identified by the Downloadable.

20. The method of claim 1 further comprising the step of examining the intended recipient userID to determine the appropriate security policy.

SOPHOS
EXHIBIT 1004 - PAGE 0370

21. The method of claim 1, further comprising the step of examining the Downloadable to determine the appropriate security policy.

22. The method of claim 20, wherein the appropriate security policy includes the default security policy.

23. The method of claim 26, further comprising the step of including a previously received Downloadable as a known Downloadable.

24. The method of claim 23, wherein the security policy identifies a Downloadable to be blocked per administrative override.

25. The method of claim 23, wherein the security policy identifies a Downloadable to be allowed per administrative override.

26. The method of claim 1, further comprising the step of comparing the Downloadable against a known Downloadable.

27. The method of claim 26, wherein the known Downloadable is hostile.

28. The method of claim 26, wherein the known Downloadable is non-hostile.

SOPHOS
EXHIBIT 1004 - PAGE 0371

29. The method of claim 2, wherein the security policy includes an access control list and further comprising the step of comparing the Downloadable security profile data against the access control list.

30. The method of claim 1, further comprising the step of informing a user upon detection of a security policy violation.

31. A system, comprising:

a security policy;

an interface for receiving a Downloadable; and

a comparator, coupled to the interface, for applying the security policy to the Downloadable to determine if the security policy has been violated.

32. The system of claim 31, wherein the Downloadable includes a Java™ applet.

33. The system of claim 31, wherein the Downloadable includes ActiveX™ control.

34. The system of claim 31, wherein the Downloadable includes a JavaScript™ script.

35. The system of claim 31, wherein the Downloadable includes a Visual Basic script.

SOPHOS
EXHIBIT 1004 - PAGE 0372

36. The system of claim 31, wherein

the Downloadable is addressed to a client; and

the security policy includes a default security policy to be applied regardless of the client to whom the Downloadable is addressed.

37. The system of claim 31, wherein

the Downloadable is addressed to a client; and

the security policy includes a specific security policy to be applied if the Downloadable is addressed to the client.

38. The system of claim 31, wherein

the Downloadable is addressed to a client belonging to a group; and

the security policy includes a specific security policy to be applied if the client belongs to a particular group.

39. The system of claim 31, further comprising an ID generator coupled to the interface for computing a Downloadable ID identifying the Downloadable.

40. The system of claim 39, wherein the ID generator prefetches all components of the Downloadable and uses all components to compute the Downloadable ID.

41. The system of claim 40, wherein the ID generator computes the digital hash of all the prefetched components.

SOPHOS
EXHIBIT 1004 - PAGE 0373

42. The system of claim 31, further comprising a policy finder for finding the security policy.

43. The system of claim 42, wherein the policy finder finds the security policy based on the user.

44. The system of claim 42 wherein the policy finder finds the security policy based on the user and the Downloadable.

45. The system of claim 42, wherein the policy finder obtains the default security policy.

46. The system of claim 31 wherein the comparator examines the security policy to determine which tests to apply.

47. The system of claim 46 wherein the comparator compares the Downloadable against a known Downloadable.

48. The system of claim 47, wherein the known Downloadable is hostile.

49. The system of claim 47, wherein the known Downloadable is non-hostile.

50. The system of claim 31, wherein the security policy identifies a Downloadable to be blocked per administrative override.

SOPHOS
EXHIBIT 1004 - PAGE 0374

167

168 51. The system of claim 31, wherein the security policy identifies a Downloadable
169 to be allowed per administrative override.

170

171 52. The system of claim 31, wherein
172 the Downloadable is addressed to a client; and
173 the comparator sends a substitute non-hostile Downloadable to the client for
174 informing the client.

175

176 53. The system of claim 31, further comprising a code scanner coupled to the
177 comparator for decomposing the Downloadable into Downloadable security profile
178 data.

179

180 54. The system of claim 53, further comprising an ACL comparator coupled to the
181 code scanner for comparing the Downloadable security profile data against an access
182 control list.

183

184 55. The system of claim 31, further comprising a certificate scanner coupled to the
185 comparator for examining the Downloadable for a certificate.

186

187 56. The system of claim 55, further comprising a certificate comparator coupled to
188 the certificate scanner for comparing the certificate against a trusted certificate.

189

SOPHOS
EXHIBIT 1004 - PAGE 0375

57. The system of claim 31, further comprising a URL comparator coupled to the comparator for comparing the URL from which the Downloadable originated against a known URL.

58. The system of claim 57, wherein the known URL identifies an untrusted URL.

59. The system of claim 57, wherein the known URL identifies a trusted URL.

60. The system of claim 31, further comprising a logical engine for responding to the results of the comparison.

61. The system of claim 31, wherein the logical engine responds according to the security policy.

62. The system of claim 31, further comprising a record-keeping engine coupled to the comparator for recording results in an event log.

63. A system, comprising:

means for receiving a Downloadable;

means for comparing the Downloadable against a security policy to determine if the security policy has been violated; and

means for discarding the Downloadable if the security policy has been violated.

SOPHOS
EXHIBIT 1004 - PAGE 0376

64. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

receiving a Downloadable;

comparing the Downloadable against a security policy to determine if the security policy has been violated; and

discarding the Downloadable if the security policy has been violated.

65. A computer-based method for generating a Downloadable ID to identify a Downloadable, comprising the steps of:

selecting Downloadable code;

performing a function on the selected Downloadable code to generate the Downloadable ID; and

storing the Downloadable ID.

66. The method of claim 65, wherein the function includes a hashing function

SOPHOS
EXHIBIT 1004 - PAGE 0377

67. The method of claim 65, wherein the Downloadable code includes a reference to a Downloadable component, and further comprising the step of fetching the component.

68. The method of claim 67, wherein the component includes the first component referenced by the Downloadable code.

69. The method of claim 65, wherein the selected Downloadable code includes all of the code included in and identified by the Downloadable.

70. The method of claim 67, further comprising the step of fetching all components referenced by the Downloadable.

SOPHOS
EXHIBIT 1004 - PAGE 0378

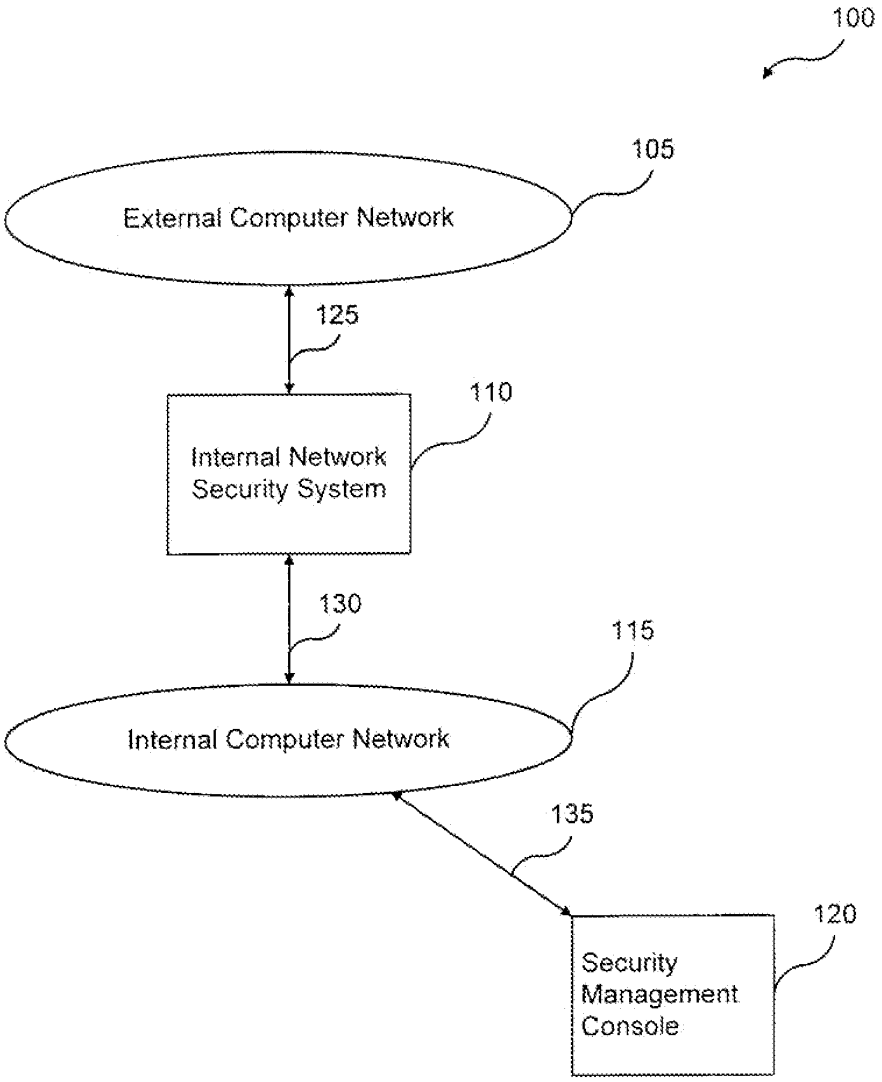

100
105
External Computer Network
125
110
Internal Network Security System
130
115
Internal Computer Network
135
120
Security Management Console

FIG. 1

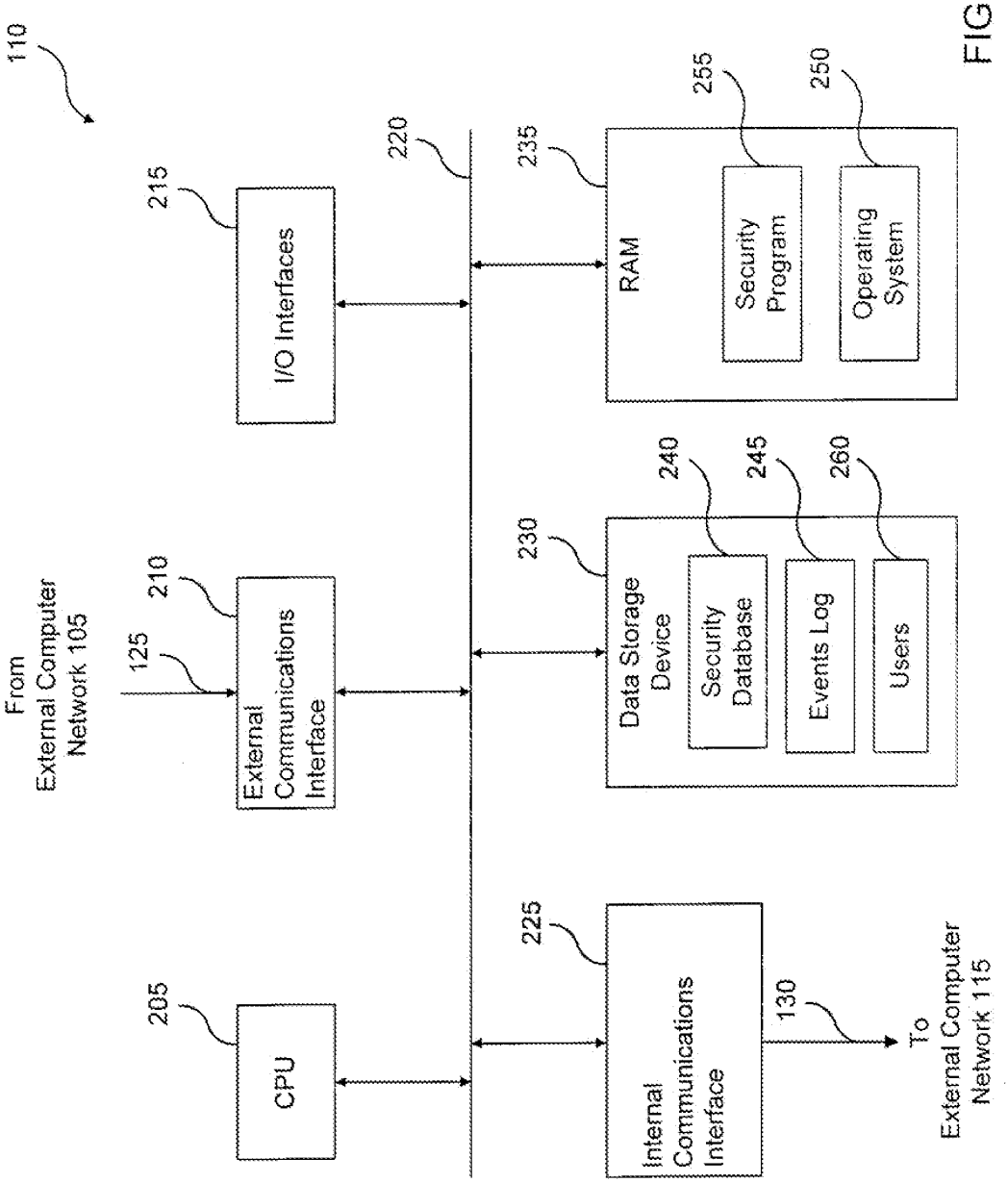


FIG. 2

SOPHOS
EXHIBIT 1004 - PAGE 0380

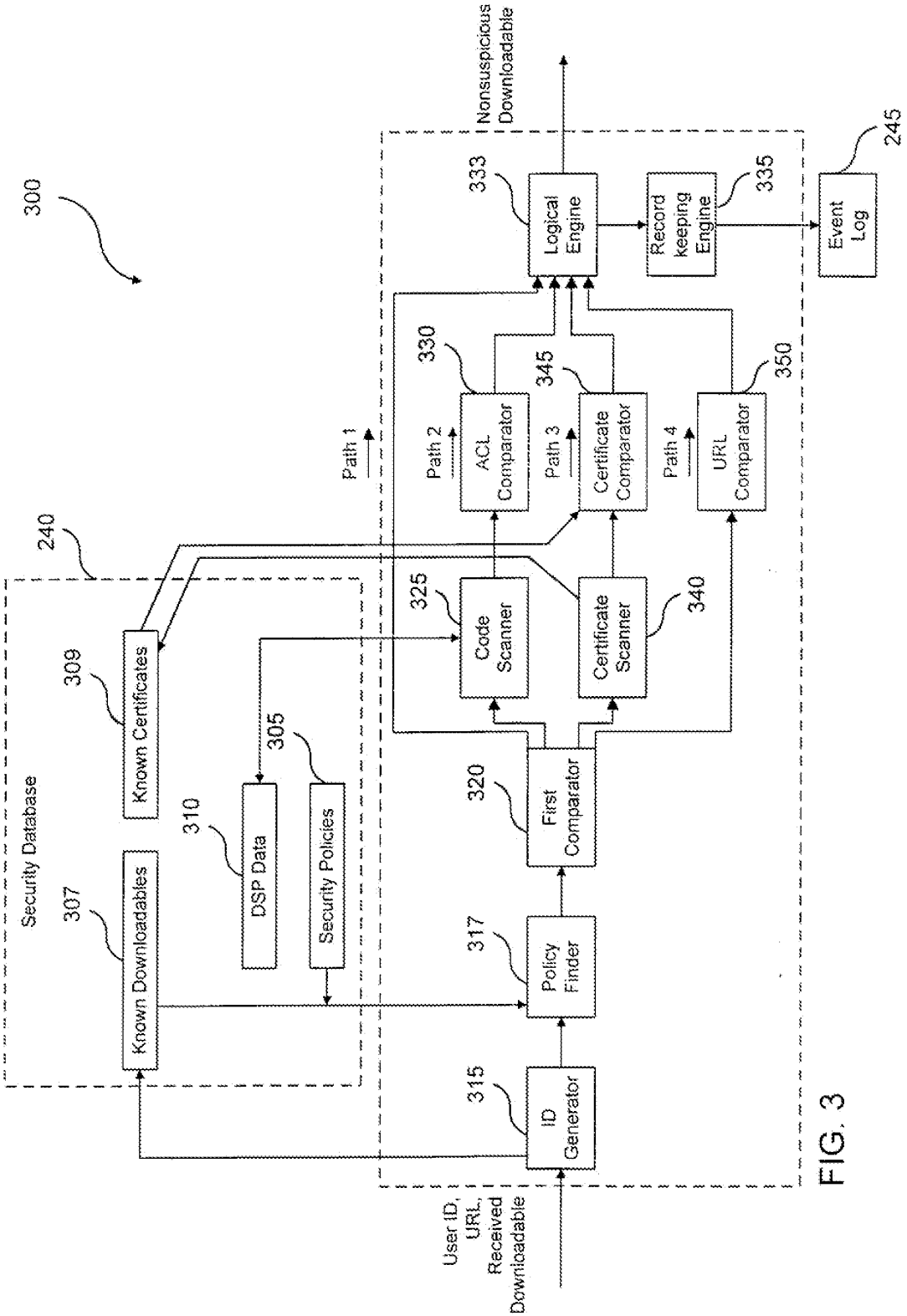


FIG. 3

SOPHOS
EXHIBIT 1004 - PAGE 0381

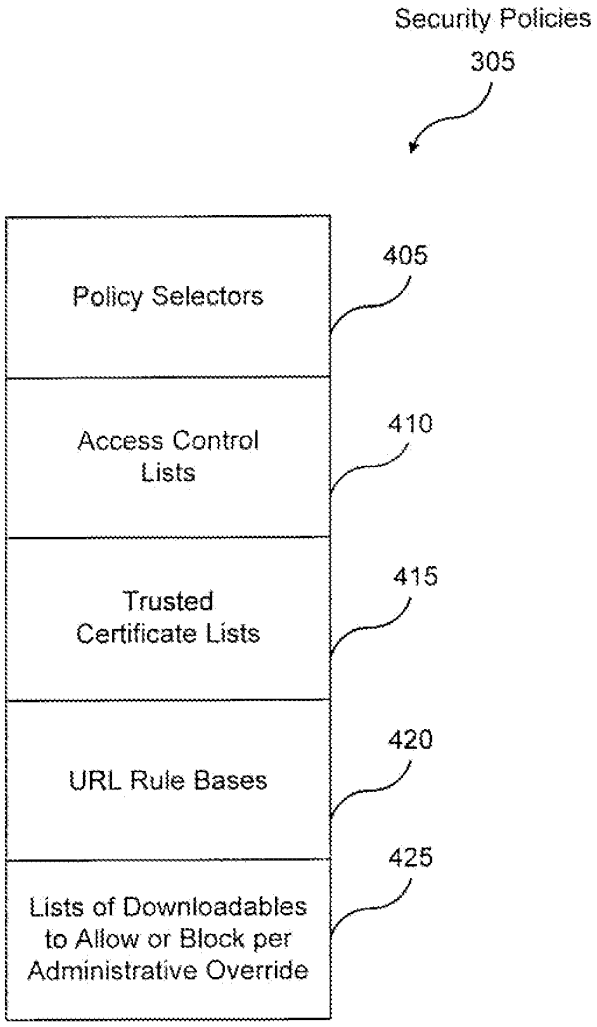

Security Policies
305
Policy Selectors
405
Access Control Lists
410
Trusted Certificate Lists
415
URL Rule Bases
420
Lists of Downloadables to Allow or Block per Administrative Override
425

FIG. 4

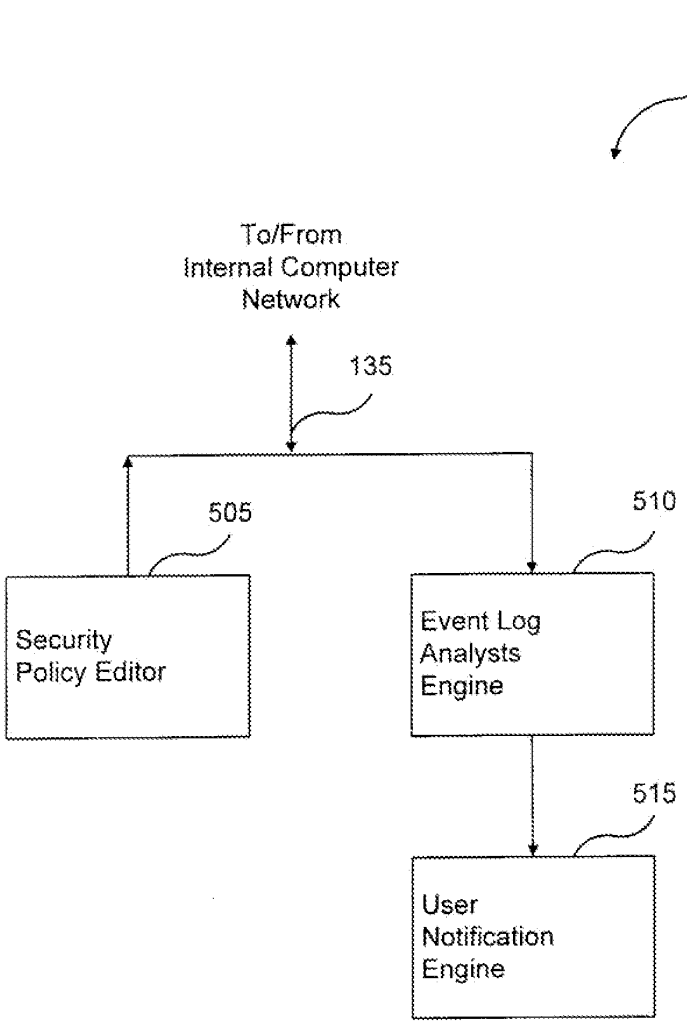

120
To/From
Internal Computer
Network
135
505
510
Security
Policy Editor
Event Log
Analysts
Engine
515
User
Notification
Engine

FIG. 5

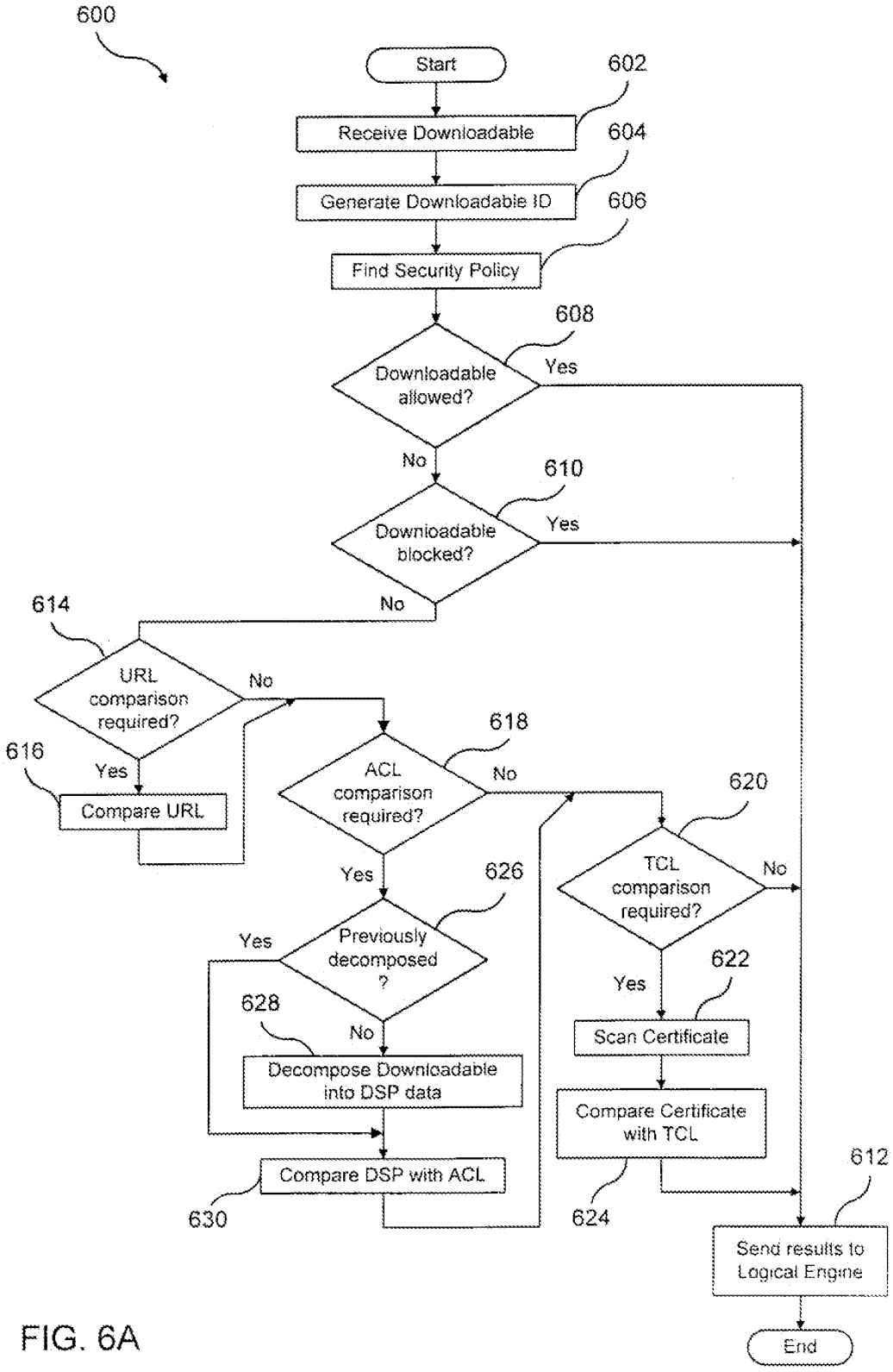

600
Start
602
Receive Downloadable
604
Generate Downloadable ID
606
Find Security Policy
608
Downloadable allowed?
Yes
No
610
Downloadable blocked?
Yes
No
614
URL comparison required?
No
Yes
616
Compare URL
618
ACL comparison required?
No
Yes
626
Previously decomposed ?
Yes
No
628
Decompose Downloadable into DSP data
Compare DSP with ACL
630
620
TCL comparison required?
No
Yes
622
Scan Certificate
Compare Certificate with TCL
624
612
Send results to Logical Engine
End

FIG. 6A

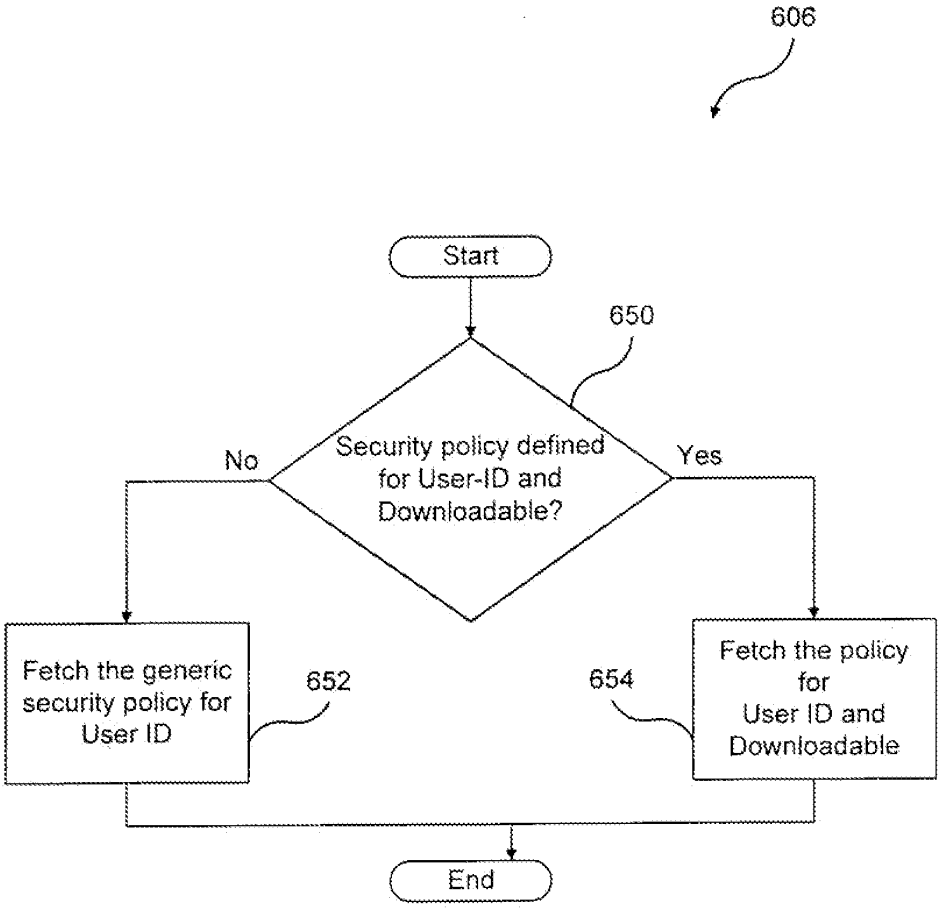

606
Start
650
Security policy defined for User-ID and Downloadable?
No
Yes
Fetch the generic security policy for User ID
652
654
Fetch the policy for User ID and Downloadable
End

FIG. 6B

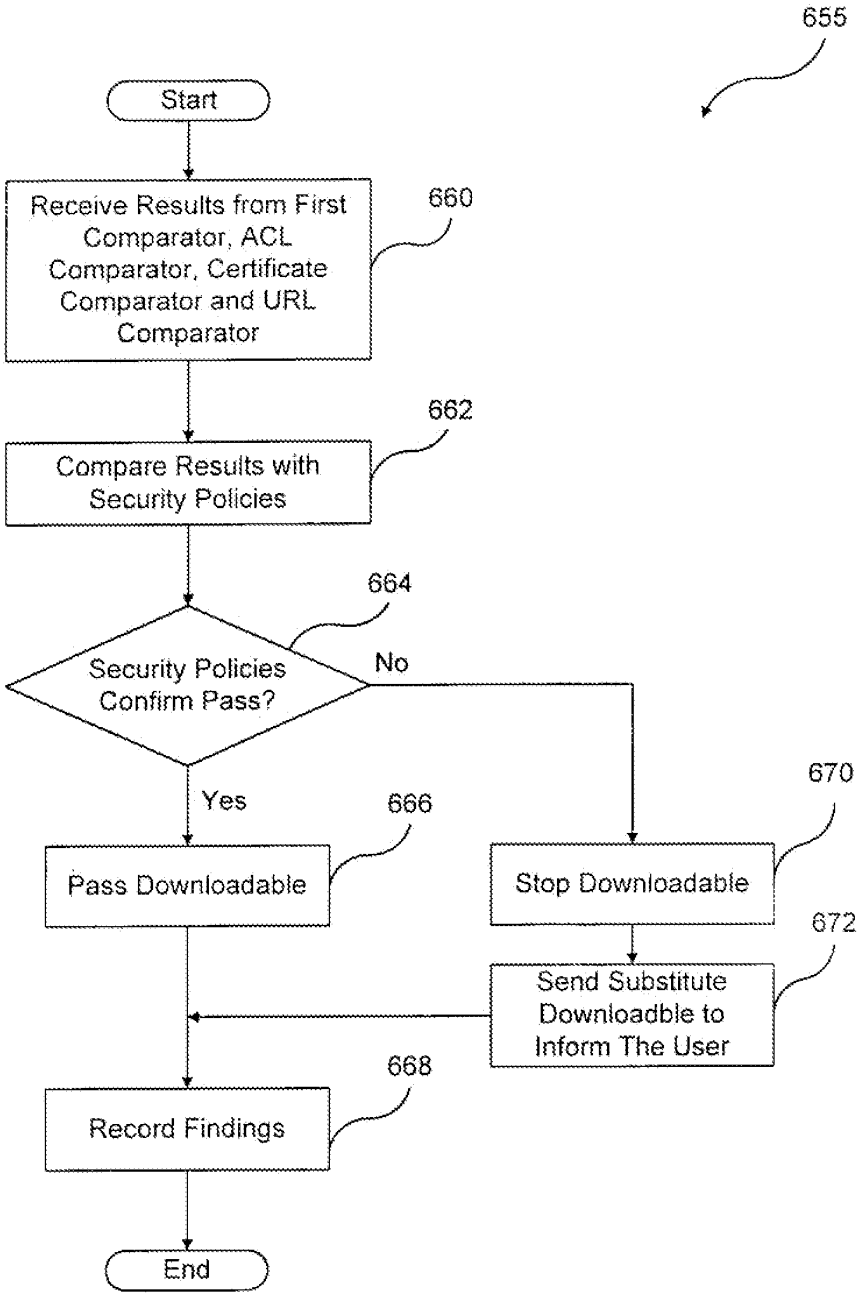

655
Start
Receive Results from First Comparator, ACL Comparator, Certificate Comparator and URL Comparator
660
Compare Results with Security Policies
662
Security Policies Confirm Pass?
664
No
Yes
Pass Downloadable
666
Stop Downloadable
670
Send Substitute Downloadble to Inform The User
672
Record Findings
668
End

FIG. 6C

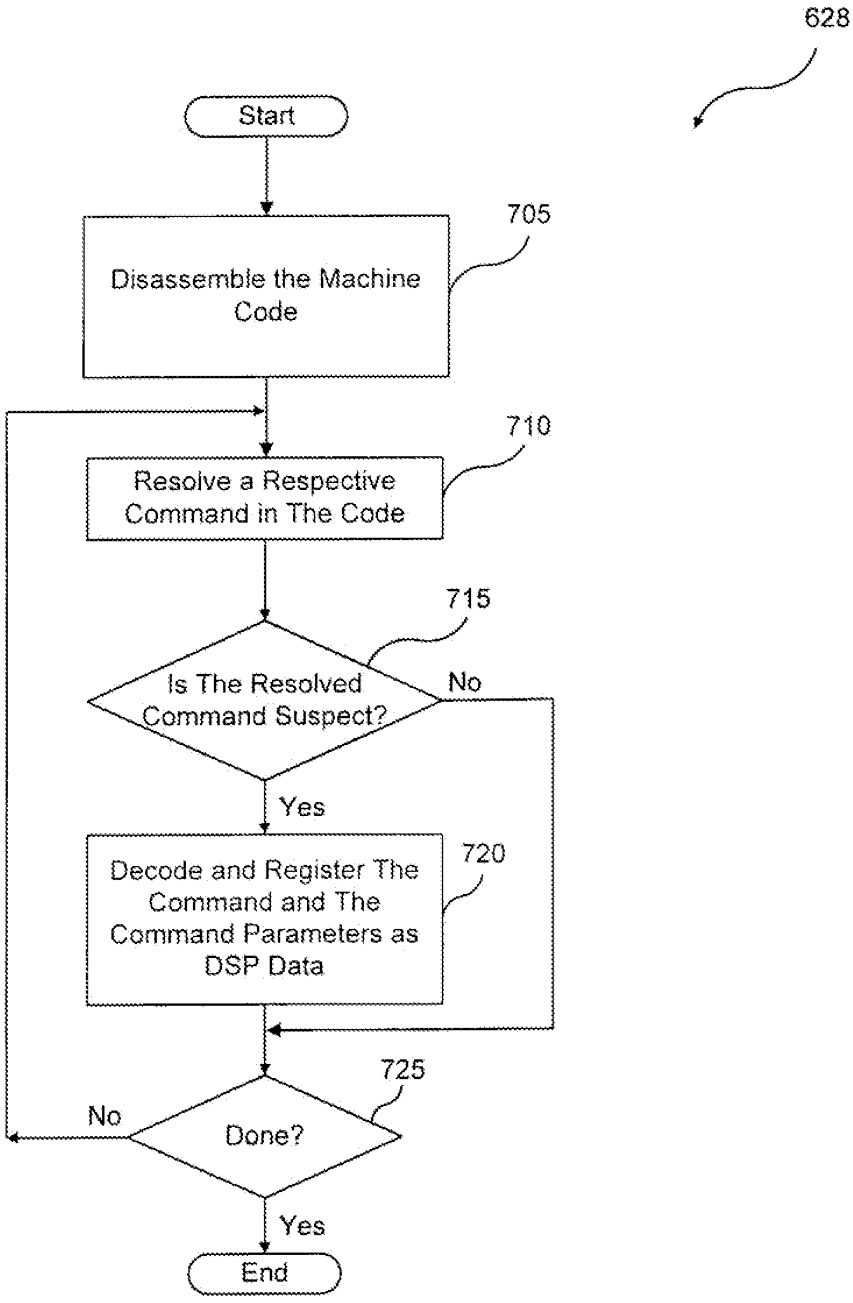

628
Start
705
Disassemble the Machine Code
710
Resolve a Respective Command in The Code
715
Is The Resolved Command Suspect?
No
Yes
720
Decode and Register The Command and The Command Parameters as DSP Data
725
Done?
No
Yes
End

FIG. 7

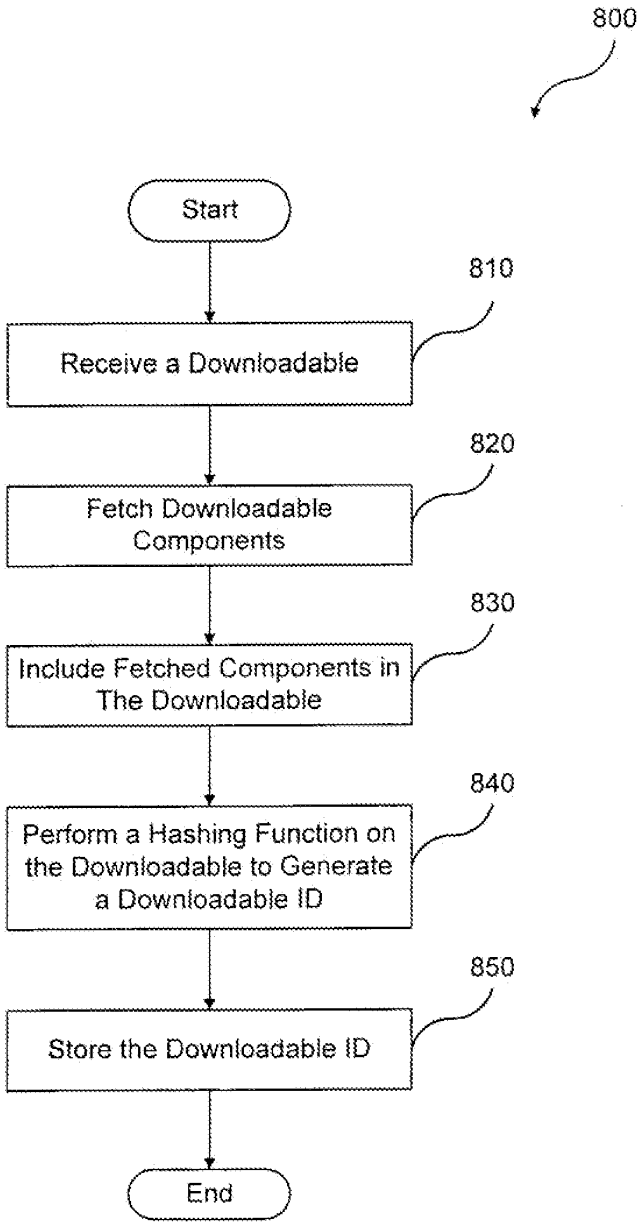

800
Start
810
Receive a Downloadable
820
Fetch Downloadable Components
830
Include Fetched Components in The Downloadable
840
Perform a Hashing Function on the Downloadable to Generate a Downloadable ID
850
Store the Downloadable ID
End

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB97/01626

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G06F 19/00, 15/18, 9/44
US CL : 395/187.01, 186, 188.01, 200.48, 200.59, 10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 395/187.01, 186, 188.01, 200.48, 200.59, 10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

NONE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	US 5,572,643 A (JUDSON) 05 November 1996, col. 2, lines 12-53, col. 3, lines 48-67, col. 4, lines 5-51, col. 7, lines 1-13	1-70
X	US 5,077,677 A (MURPHY ET AL) 31 December 1991, COL. 2, LINES 60-66, COL. 19, LINES 8-16	10, 35
X,E	US 5,692,047 A (MCMANIS) 25 November 1997, col. 3, lines 14-29.	66

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 25 MARCH 1998	Date of mailing of the international search report 14 MAY 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer for PIERRE EDDY ELISCA Telephone No. (703) 305-3987

Form PCT/ISA/210 (second sheet)(July 1992)★

SOPHOS
EXHIBIT 1004 - PAGE 0389

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL05/00915

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 11/30
US CL : 726/22, 23, 24
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 726/22, 23, 24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,487,666 B1 (SHANKLIN et al) 26 November 2002, see entire document	1-43

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 February 2006 (05.02.2006)	03 MAR 2006
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Ayaz Sheikh Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL05/00915

Continuation of B. FIELDS SEARCHED Item 3:
BRS (files: USPAT, US PGPUB, USOCR, DERWENT, IBM TDB, JPO, EPO)

search terms: token, signature, expression, trait, rule, policy, exploit, malicious, suspicious, attack, intrusion, parse, parsed, parser, parsing

SOPHOS
EXHIBIT 1004 - PAGE 0391

REC'D 07 MAR 2006
WIPO PCT

From the
INTERNATIONAL SEARCHING AUTHORITY

PATENT COOPERATION TREATY

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

To:
TALLY EITAN
EITAN LAW GROUP
P.O. BOX 2081
INDUSTRIAL ZONE
HERZLIA, 46120
ISRAEL

Applicant's or agent's file reference P-9039-PC	Date of mailing (*day/month/year*) 03 MAR 2006 **FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date (*day/month/year*)	Priority date (*day/month/year*)
PCT/IL05/00915	24 August 2005 (24.08.2005)	30 August 2004 (30.08.2004)

International Patent Classification (IPC) or both national classification and IPC
IPC(7): G06F 11/30 and US Cl.: 726/22, 23, 24

Applicant
FINJAN SOFTWARE, LTD.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I — Basis of the opinion
- ☐ Box No. II — Priority
- ☐ Box No. III — Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV — Lack of unity of invention
- ☒ Box No. V — Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI — Certain documents cited
- ☐ Box No. VII — Certain defects in the international application
- ☐ Box No. VIII — Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(*b*) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	05 February 2006 (05.02.2006)	Ayaz Sheikh for Telephone No. 703-305-3900

Form PCT/ISA/237 (cover sheet) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IL05/00915

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:

☒ the international application in the language in which it was filed

☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

SOPHOS
EXHIBIT 1004 - PAGE 0393

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IL05/00915

Box No. V Reasoned statement under Rule 43 *bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims NONE	YES
	Claims 1-43	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-43	NO
Industrial applicability (IA)	Claims 1-43	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

SOPHOS
EXHIBIT 1004 - PAGE 0394

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:
Claims 1-43 lack novelty under PCT Article 33(2) as being anticipated by Shanklin et al, U.S. Patent 6,487,666.

1. A method for scanning content, comprising: identifying tokens within an incoming byte stream, the tokens being lexical constructs for a specific language; identifying patterns of tokens; generating a parse tree from the identified patterns of tokens; and identifying the presence of potential exploits within the parse tree, wherein said identifying tokens, identifying patterns of tokens, and identifying the presence of potential exploits are based upon a set of rules for the specific language (see col. 2, lines 3-15; col. 3, lines 54-60; col. 4, lines 40-48; and col. 5, lines 23-28).
2. The method of claim 1 further comprising converting the incoming byte stream to a reduced set of character codes (col. 2, lines 3-15).
3. The method of claim 1 wherein further comprising decoding character sequences according to an escape encoding (col. 2, lines 3-15).
4. The method of claim 1 wherein said generating a parse tree is based upon a shift-and-reduce algorithm (col. 3, lines 54-60).
5. The method of claim 1 wherein the set of rules expresses exploits in terms of patterns of tokens (col. 2, lines 3-15).
6. The method of claim 1 wherein the set of rules includes actions to be performed when corresponding patterns are matched (col. 2, lines 3-15).
7. The method of claim 1 wherein the specific language is JavaScript (col. 2, lines 15-21).
8. The method of claim 1 wherein the specific language is Visual Basic VBScript (col. 2, lines 15-21).
9. The method of claim 1 wherein the specific language is HTML (col. 2, lines 15-21).
10. The method of claim 1 wherein the specific language is Uniform Resource Identifier (URI)(col. 2, lines 45-48).
11. The method of claim 1 for scanning a first type of content that has a second type of content embedded therewithin, further comprising recursively invoking another method in accordance with claim 1, for scanning the second type of content (col. 2, lines 3-15).
12. A system for scanning content, comprising: a tokenizer for identifying tokens within an incoming byte stream, the tokens being lexical constructs for a specific language; a parser operatively coupled to said tokenizer for identifying patterns of tokens, and generating a parse tree therefrom; and an analyzer operatively coupled to said parser for analyzing the parse tree and identifying the presence of potential exploits therewithin, wherein said tokenizer, said parser and said analyzer use a set of rules for the specific language to identify tokens, patterns and potential exploits, respectively (see col. 2, lines 3-15; col. 3, lines 54-60; col. 4, lines 40-48; and col. 5, lines 23-28).
13. The system of claim 12 further comprising a pre-scanner for identifying content that is innocuous (col. 2, lines 3-15).
14. The system of claim 12 wherein said tokenizer comprises a normalizer for converting the incoming byte stream to a reduced set of character codes (col. 2, lines 3-15).
15. The system of claim 12 wherein said tokenizer comprises a decoder for decoding character sequences according to an escape encoding (col. 2, lines 3-15).
16. The system of claim 12 wherein said parser generates the parse tree using a shift-and-reduce algorithm (col. 3, lines

SOPHOS
EXHIBIT 1004 - PAGE 0395

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

54-60).
17. The system of claim 12 further comprising a pattern-matching engine operatively coupled to said parser and to said analyzer, for matching a pattern within a sequence of tokens (col. 3, lines 54-60).
18. The system of claim 17 wherein the pattern is represented as a finite-state machine (col. 2, lines 3-15).
19. The system of claim 17 wherein the pattern is represented as a pattern expression tree (col. 2, lines 3-15).
20. The system of claim 17 wherein patterns are merged into a single deterministic finite automaton (DFA)(col. 2, lines 3-15).
21. The system of claim 12 wherein the set of rules expresses exploits in terms of patterns of tokens (col. 2, lines 3-15).
22. The system of claim 12 wherein the set of rules includes actions to be performed when corresponding patterns are matched (col. 2, lines 3-15).
23. The system of claim 22 further comprising a scripting engine for implementing the actions to be performed (col. 2, lines 3-15).
24. The system of claim 12 wherein the specific language is JavaScript (col. 2, lines 15-21).
25. The system of claim 12 wherein the specific language is Visual Basic script (col. 2, lines 15-21).
26. The system of claim 12 wherein the specific language is HTML (col. 2, lines 15-21).
27. The system of claim 12 wherein the specific language is Uniform Resource Identifier (URI)(col. 2, lines 45-48).
28. A computer-readable storage medium storing program code for causing a computer to perform the steps of identifying tokens within an incoming byte stream, the tokens being lexical constructs for a specific language; identifying patterns of tokens; generating a parse tree from the identified patterns of tokens; and identifying the presence of potential exploits within the parse tree, wherein said identifying tokens, identifying patters of tokens, and identifying the presence of potential exploits are based upon a set of rules for the specific language (see col. 2, lines 3-15; col. 3, lines 54-60; col. 4, lines 40-48; and col. 5, lines 23-28).
29. A method for scanning content, comprising expressing an exploit in terms of patterns of tokens and rules, where tokens are lexical constructs of a specific programming language, and rules are sequences of tokens that form programmatical constructs; and parsing an incoming byte source to determine if an exploit is present therewithin, based on said expressing (see col. 2, lines 3-15; col. 3, lines 54-60; col. 4, lines 40-48; and col. 5, lines 23-28).
30. The method of claim 29 further comprising generating a parse tree for the incoming byte source, the nodes of the parse tree corresponding to tokens and rules (col. 3, lines 54-60).
31. The method of claim 30 wherein nodes of the parse tree corresponding to rules are positioned as parent nodes, the children of which correspond to the sequences of tokens that correspond to the rules (col. 3, lines 54-60).
32. The method of claim 31 wherein a new parent node is added to the parse tree if a rule is matched (col. 3, lines 54-60).
33. The method of claim 32 wherein said parsing determines if an exploit is present within the incoming byte source when a new parent node is added to the parse tree (col. 3, lines 54-60).
34. The method of claim 33 wherein tokens and rules have names associated therewith, and further comprising assigning values to nodes in the parse tree, the value of a node corresponding to a token being the name of the corresponding token, and the value of a node corresponding to a rule being the name of the corresponding rule (col. 3, lines 54-60).
35. The method of claim 34 further comprising storing an indicator for the matched rule in the new parent node of the parse tree, if said parsing determines the presence of the matched rule (col. 3, lines 54-60).
36. A system for scanning content, comprising a parser for parsing an incoming byte source to determine if an exploit is present therewithin, based on a formal description of the exploit expressed in terms of patterns of tokens and rules, where tokens are lexical constructs of a specific programming language, and rules are sequences of tokens that form programmatical constructs (see col. 2, lines 3-15; col. 3, lines 54-60; col. 4, lines 40-48; and col. 5, lines 23-28).
37. The system of claim 36 wherein said parser comprises a tree generator for generating a parse tree for the incoming byte source, the nodes of the parse tree corresponding to tokens and rules (col. 3, lines 54-60).
38. The system of claim 37 wherein nodes of the parse tree corresponding to rules are positioned as parent nodes, the children of which correspond to the sequences of tokens that correspond to the rules (col. 3, lines 54-60).
39. The system of claim 38 wherein said tree generated adds a new parent node to the parse tree if a rule is matched (col. 3, lines 54-60).
40. The system of claim 39 wherein said parser determines if a matched rule is present within the incoming byte source when said tree generator adds a new parent node to the parse tree (col. 3, lines 54-60).
41. The system of claim 40 wherein tokens and rules have names associated therewith, and wherein said tree generator assigns value to nodes in the parse tree, the value of a node corresponding to a token being the name of the corresponding token, and the value of a node corresponding to a rule being the name of the corresponding rule (col. 3, lines 54-60).
42. The system of claim 41 wherein said tree generator stores an indicator for the matched rule in the new parent node of the parse tree, if said parser determines the presence of the matched rule (col. 3, lines 54-60).
43. A computer-readable storage medium storing program code for causing a computer to perform the steps of expressing an exploit in terms of patterns of tokens and rules, where tokens are lexical constructs of a specific programming language, and rules are sequences of tokens that form programmatical constructs; and parsing an incoming byte source to determine if an exploit is present therewithin, based on said expressing (see col. 2, lines 3-15; col. 3, lines 54-60; col. 4, lines 40-48; and col. 5, lines 23-28).

SOPHOS
EXHIBIT 1004 - PAGE 0396

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 01/01138

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 983 348 A (JI SHUANG) 9 November 1999 (1999-11-09) cited in the application	30-64, 67-76
Y	column 1, line 9 - line 25	1-5, 11-13, 15-19, 24-29, 65,66
	column 2, line 62 -column 3, line 56 column 3, line 65 -column 5, line 15 column 6, line 38 -column 8, line 15 figures 1,2	

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 September 2002	20/09/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Arbutina, L

Form PCT/ISA/210 (second sheet) (July 1992)

SOPHOS
EXHIBIT 1004 - PAGE 0397

INTERNATIONAL SEARCH REPORT

Inter Application No
PCT/IB 01/01138

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 623 600 A (JI SHUANG ET AL) 22 April 1997 (1997-04-22) abstract column 7, line 29 -column 8, line 38	1-5, 11-13, 15-19, 24-29
Y	US 5 974 549 A (GOLAN GILAD) 26 October 1999 (1999-10-26) cited in the application abstract column 5, line 37 -column 6, line 29	65,66

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte . . lication No
PCT/IB 01/01138

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5983348 A	09-11-1999	AU 8822998 A	29-03-1999
		WO 9913402 A1	18-03-1999
		US 6272641 B1	07-08-2001
US 5623600 A	22-04-1997	AU 2001997 A	17-04-1997
		DE 19680539 T0	11-12-1997
		EP 0852762 A1	15-07-1998
		GB 2309561 A	30-07-1997
		JP 11513153 T	09-11-1999
		WO 9712321 A1	03-04-1997
		US 5889943 A	30-03-1999
US 5974549 A	26-10-1999	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

PATENT COOPERATION TREATY

PCT

REC'D 31 DEC 2002
WIPO PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

(Rationalised Report according to the Notice of the President of the EPO published in the OJ11/2001)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
134943.0 SZ		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/IB 01/01138	17/05/2001	17/05/2000
International Patent Classification (IPC) or national classification and IPC		
G06F1/00		
Applicant		
FINJAN SOFTWARE, LTD.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This **REPORT** consists of a total of 2 sheets, including this cover sheet.

   ☐ This report is also accompanied by **ANNEXES**, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consists of a total of _____ sheets.

3. This report contains indications relating to the following items:

   I ☒ Basis of the report

   II ☐ Priority

   III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

   IV ☐ Lack of unity of invention

   V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

   VI ☐ Certain documents cited

   VII ☐ Certain defects in the international application

   VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
30/11/2001	19/12/2002
Name and mailing address of the IPEA/ European Patent Office D-80298 Munich Tel. (+49-89) 2399-0, Tx: 523656 epmu d Fax: (+49-89) 2399-4465	Authorized officer NESSMANN C A Tel. (+49-89) 2399 2828

EUROPÄISCHES PATENTAMT - EUROPEAN PATENT OFFICE - OFFICE EUROPÉEN DES BREVETS

SOPHOS
EXHIBIT 1004 - PAGE 0400

I. Basis of the report

The basis of this international preliminary examination is the application as originally filed.

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability

In light of the documents cited in the international search report, it is considered that the invention as defined in at least some of the claims does not appear to meet the criteria mentioned in Article 33(1) PCT, i.e. does not appear to be novel and/or to involve an inventive step (see international search report, in particular the documents cited X and/or Y and corresponding claim references).

SOPHOS
EXHIBIT 1004 - PAGE 0401

PTO/SB/30 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

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

Application Number	13290708
Filing Date	2011-11-07
First Named Inventor	EDERY, Yigal
Art Unit	2431
Examiner Name	REVAK, Christopher A
Attorney Docket Number	FIN0001-CON1-CIP1-CON4

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 NonPatent Literature

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. _____.

      i. ☑ RCE fee required under 37 CFR 1.17(e)

      ii. ☑ Extension of time fee (37 CFR 1.136 and 1.17)

      iii. ☑ Other Credit Card Payment via EFS-Web

   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	/Dawn-Marie Bey/	Date	05/07/2013
Name (Print/Type)	Dawn-Marie Bey	Registration No.	44,442

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			
Name (Print/Type)		Date	

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.

PTO/SB/30 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Instruction Sheet for RCEs

(not to be submitted to the USPTO)

NOTES:

An RCE is not a new application, and filing an RCE will not result in an application being accorded a new filing date.

Filing Qualifications:

The application must be a utility or plant application filed on or after June 8, 1995. The application cannot be a provisional application, a utility or plant application filed before June 8, 1995, a design application, or a patent under reexamination. See 37 CFR 1.114(e).

Filing Requirements:

Prosecution in the application must be closed. Prosecution is closed if the applicat ion is under appeal, or the last Office action is a final action, a notice of allowance, or an action that otherwise closes prosecution in the application (e.g., an Office action under *Ex parte Quayle*). See 37 CFR 1.114(b).

A submission and a fee are required at the time the RCE is filed. If reply to an Office action under 35 U.S.C. 132 is outstanding (e.g., the application is under final rejection), the submission must meet the reply requirements of 37 CFR 1.111. If there is no outstanding Office action, the submission can be an information disclosure statement, an amendment, new arguments, or new evidence. See 37 CFR 1.114(c). The submission may be a previously filed amendment (e.g., an amendment after final rejection).

WARNINGS:

Request for Suspension of Action:

All RCE filing requirements must be met before suspension of action is granted. A request for a suspension of action under 37 CFR 1.103(c) does not satisfy the submission requirement and does not permit the filing of the required submission to be suspended.

Improper RCE will NOT toll Any Time Period:

Before Appeal - If the RCE is improper (e.g., prosecution in the application is not closed or the submission or fee has not been filed) and the application is not under appeal, the time period set forth in the last Office action will continue to run and the application will be abandoned after the statutory time period has expired if a reply to the Office action is not timely filed. No additional time will be given to correct the improper RCE.

Under Appeal - If the RCE is improper (e.g., the submission or the fee has not been filed) and the application is under appeal, the improper RCE is effective to withdraw the appeal. Withdrawal of the appeal results in the allowance or abandonment of the application depending on the status of the claims. If there are no allowed claims, the application is abandoned. If there is at least one allowed claim, the application will be passed to issue on the allowed claim(s). See MPEP 1215.01.

See MPEP 706.07(h) for further information on the RCE practice.

SOPHOS
EXHIBIT 1004 - PAGE 0403

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.

Electronic Patent Application Fee Transmittal

Application Number:	13290708
Filing Date:	07-Nov-2011
Title of Invention:	Malicious Mobile Code Runtime Monitoring System and Methods
First Named Inventor/Applicant Name:	Yigal Mordechai Edery
Filer:	Dawn-Marie Bey./Amanda Bayliss
Attorney Docket Number:	FIN0001-CON1-CIP1-CON4

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with $0 paid	1251	1	200	200

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for Continued Examination	1801	1	1200	1200
		Total in USD ($)		**1400**

Electronic Acknowledgement Receipt

EFS ID:	15714222
Application Number:	13290708
International Application Number:	
Confirmation Number:	4120
Title of Invention:	Malicious Mobile Code Runtime Monitoring System and Methods
First Named Inventor/Applicant Name:	Yigal Mordechai Edery
Customer Number:	74877
Filer:	Dawn-Marie Bey./Amanda Bayliss
Filer Authorized By:	Dawn-Marie Bey.
Attorney Docket Number:	FIN0001-CON1-CIP1-CON4
Receipt Date:	07-MAY-2013
Filing Date:	07-NOV-2011
Time Stamp:	16:07:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1400
RAM confirmation Number	2839
Deposit Account	
Authorized User	

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)	FIN0001CON1CIP1CON4_RCE_Submission.pdf	59803 67ea6dc6e2760cd86e92acb8e085a9526f1df6ee	no	6
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2	Affidavit-Rule 131-pre-AIA (FTI) ONLY	Finjan_Shlomo_Declaration.pdf	697545 e05598b5c14317c64bd3fb452dcd478ca27be91f	no	3
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	FIN0001_CON1_CIP1_CON4_IDS1.pdf	151528 8c4ec1b91b729d7d3987475b083208b277b335d8	no	18
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Information Disclosure Statement (IDS) Form (SB08)	FIN0001_CON1_CIP1_CON4_IDS2.pdf	114599 07858efed5fee7709c5dcf672691c75ed1e38acb	no	8
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
5	Information Disclosure Statement (IDS) Form (SB08)	FIN0001_CON1_CIP1_CON4_IDS3.pdf	113456 4ed0befaec4aa3644a5a9242ad0e04094fd10e64	no	8
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
6	Information Disclosure Statement (IDS) Form (SB08)	FIN0001_CON1_CIP1_CON4_IDS4.pdf	122747 81650ce8fa565ecbb6edc814ce2f5c7d47976e57	no	8
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
7	Information Disclosure Statement (IDS) Form (SB08)	FIN0001_CON1_CIP1_CON4_IDS5.pdf	113122 a0c92b4dcced53ee90545b183560291b2cf4af81	no	6
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
8	Foreign Reference	1ForeignReference.pdf	407110 58fbcfb84da2d51eb09f363c02d6f6d239e6259b	no	8

Warnings:					
Information:					
9	Foreign Reference	2ForeignReference.pdf	2260772 beec6c66c081838b23e03bb95e1f04c72a69df8d	no	17
Warnings:					
Information:					
10	Foreign Reference	3ForeignReference.pdf	881433 98fea7e2984cb997512b0d275d646ff74bb59883	no	22
Warnings:					
Information:					
11	Foreign Reference	4ForeignReference.pdf	6319570 93d4f13c153a824cb3c2b5d1e21e94558b13d076	no	75
Warnings:					
Information:					
12	Foreign Reference	5ForeignReference.pdf	61959 e39fb1c049417d0f2b732b111704ffccfbebc34a	no	1
Warnings:					
Information:					
13	Foreign Reference	6ForeignReference.pdf	1046946 40ca370993ac7dd61a94d26e621e1ef10d9a9ba8	no	27
Warnings:					
Information:					
14	Foreign Reference	7ForeignReference.pdf	62516 2a548394fd2fe6b8003c3200dc498683363f23ea	no	1
Warnings:					
Information:					
15	Foreign Reference	8ForeignReference.pdf	4085432 c311aa5356ca7554c05e502aba98493b8d188b26	no	41
Warnings:					
Information:					
16	Non Patent Literature	1NonPatentLiterature.pdf	172850 becc368120cb61bd0fadf0ad08e8098f66211ea3	no	4
Warnings:					
Information:					
17	Non Patent Literature	2NonPatentLiterature.pdf	572697 7dc8a97f24b6a02226749b306a01ad93b7dd930b	no	7

Warnings:					
Information:					
18	Non Patent Literature	3NonPatentLiterature.pdf	56363 748aed74a5e1e4650fbe1eaa780cfd335e45327e	no	1
Warnings:					
Information:					
19	Non Patent Literature	4NonPatentLiterature.pdf	103677 074db5818dc947bf978f46131c5b8ff9af6b561b	no	3
Warnings:					
Information:					
20	Non Patent Literature	5NonPatentLiterature.pdf	6608384 6bd901abfdf03573136a0d926086d9eaea8031ce	no	85
Warnings:					
Information:					
21	Non Patent Literature	6NonPatentLiterature.pdf	4311010 c785875643525e768f5656aed51cffd95f3521b6	no	58
Warnings:					
Information:					
22	Non Patent Literature	7NonPatentLiterature.pdf	3586736 360bd0003f15ff4c66859364c99932078e2bf2b8	no	48
Warnings:					
Information:					
23	Non Patent Literature	8NonPatentLiterature.pdf	754533 1ef448f178023e0e9bc74df1f1a25fbce493dd23	no	25
Warnings:					
Information:					
24	Non Patent Literature	9NonPatentLiterature.pdf	144686 4f4d0c58e6be8042cb1d9fccf10bc4c69e7e029b	no	4
Warnings:					
Information:					
25	Non Patent Literature	10NonPatentLiterature.pdf	3510452 a9a733c12fd07cc39ea4a91898072806a658ab3b	no	38
Warnings:					
Information:					
26	Non Patent Literature	11NonPatentLiterature.pdf	3962113 a6b109eebcb09d48572469352fedfcb90446d6bb	no	46

Warnings:					
Information:					
27	Non Patent Literature	12NonPatentLiterature.pdf	4533180 fef57b85d846a46c464bacbba30fbb3eb0570144	no	45
Warnings:					
Information:					
28	Non Patent Literature	13NonPatentLiterature.pdf	2695813 8ddff9cc50fbb767ed2d8f7d36b04fd58fb16ac7	no	37
Warnings:					
Information:					
29	Non Patent Literature	14NonPatentLiterature.pdf	383387 ac716daacbfb9116ddf5d63db746de4e570886ce	no	6
Warnings:					
Information:					
30	Non Patent Literature	15NonPatentLiterature.pdf	2330711 33804b258c910d6f4c47a61528c2bae8996d2be1	no	23
Warnings:					
Information:					
31	Non Patent Literature	16NonPatentLiterature.pdf	322291 9e02ea1f4af25faf19357028067a8eb1d85103ff	no	5
Warnings:					
Information:					
32	Non Patent Literature	17NonPatentLiterature.pdf	9158745 ca2f987c7a20c00b08853e3a9532595ef5db8d76	no	113
Warnings:					
Information:					
33	Non Patent Literature	18NonPatentLiterature.pdf	7101909 ffbfeb306e30be5a693ff033a1a204063b6737af	no	113
Warnings:					
Information:					
34	Non Patent Literature	19NonPatentLiterature.pdf	14554072 e2f6c0588fe2f2b9d00096fae2f2ab5e61495864	no	127
Warnings:					
Information:					
35	Non Patent Literature	19BNonPatentLiterature.pdf	12311500 186764945843ea37a0b3e3f4bddbd2bdef372324	no	128

Warnings:					
Information:					
36	Non Patent Literature	20ANonPatentLiterature.pdf	647838 48a8bb2c0eaffc64a9fa72c187bce031cc2e5006	no	22
Warnings:					
Information:					
37	Non Patent Literature	20BNonPatentLiterature.pdf	270945 d43e2e512c72fd87797650c285e1210742d338dd	no	8
Warnings:					
Information:					
38	Non Patent Literature	21NonPatentLiterature.pdf	930304 ff6244863f853ba45a588cf2d958f02ec86ab1cc	no	18
Warnings:					
Information:					
39	Non Patent Literature	22NonPatentLiterature.pdf	7319677 4138c4eefffdc64a3e1266c38743a05a507db17d	no	6
Warnings:					
Information:					
40	Non Patent Literature	23NonPatentLiterature.pdf	3589267 3112ec8f3f97f6ff000f0859167462d331471d2a	no	52
Warnings:					
Information:					
41	Non Patent Literature	24NonPatentLiterature.pdf	233831 32618c91e901dc5f069ca6b80ef18ff8aabecbba	no	5
Warnings:					
Information:					
42	Non Patent Literature	25ANonPatentLiterature.pdf	10795459 cb2f0b5c52bfaf8909be77cc0675cd6222907677	no	231
Warnings:					
Information:					
43	Non Patent Literature	25BNonPatentLiterature.pdf	11671512 585793245ab0f092b42a7d38a9879ad8f8855e9b	no	233
Warnings:					
Information:					
44	Non Patent Literature	25CNonPatentLiterature.pdf	11363711 1701ad51d893d51192f000b2cde4dbd9494e97aa	no	233

Warnings:					
Information:					
45	Non Patent Literature	25DNonPatentLiterature.pdf	12246204 d0a63c6097a572b8ad69ec0b10fd2a54cf41d204	no	230
Warnings:					
Information:					
46	Non Patent Literature	26NonPatentLiterature.pdf	63604 7e84a7937d3b2fd876ff1fd74eac901bc37a0afb	no	2
Warnings:					
Information:					
47	Non Patent Literature	27NonPatentLiterature.pdf	285981 404aa705e5ce79aa8b7c1e103077d19dbb97082b	no	5
Warnings:					
Information:					
48	Non Patent Literature	28NonPatentLiterature.pdf	83063 0cca8c738451327fc265e3c27be3b96cb592cd98	no	3
Warnings:					
Information:					
49	Non Patent Literature	29NonPatentLiterature.pdf	72888 64c72fe42c25202ac570fd4ef7c3cac86b68b65b	no	2
Warnings:					
Information:					
50	Non Patent Literature	30NonPatentLiterature.pdf	651880 ef7d7da30ae26a3e54508658987417fb8834fa28	no	18
Warnings:					
Information:					
51	Non Patent Literature	31NonPatentLiterature.pdf	235083 7488617bc24989d2e23c6d368eae65b3e802dd5e	no	4
Warnings:					
Information:					
52	Non Patent Literature	32NonPatentLiterature.pdf	181849 3501f64163c6aacdd6763751ac0897a1c0f0791a	no	5
Warnings:					
Information:					
53	Non Patent Literature	33NonPatentLiterature.pdf	259144 221318c66951913414749d5f58b2a53e75edb2a0	no	8

Warnings:					
Information:					
54	Non Patent Literature	34NonPatentLiterature.pdf	158062 5778cd81aab2f5a998170853065a9141fcf721bd	no	7
Warnings:					
Information:					
55	Non Patent Literature	35NonPatentLiterature.pdf	91635 4ff9955800ed6234b8f1b5a2be81bb75bd3c9ec9	no	4
Warnings:					
Information:					
56	Non Patent Literature	36NonPatentLiterature.pdf	90732 5d17d27399c960cdf1a333a511b22d323eadb163	no	3
Warnings:					
Information:					
57	Non Patent Literature	37NonPatentLiterature.pdf	907433 b51f867e48463cdcbc98b7187545199347bf1465	no	38
Warnings:					
Information:					
58	Non Patent Literature	38NonPatentLiterature.pdf	5537275 ca9c148e6ca1686d178c42c1da458dcd2f2abecb	no	112
Warnings:					
Information:					
59	Transmittal Letter	FIN0001_CON1_CIP1_CON4_RCE_Transmittal.pdf	192324 fb980e543167e642743cce95f92aeed1ceb40c08	no	3
Warnings:					
Information:					
60	Fee Worksheet (SB06)	fee-info.pdf	32197 005075f2a17c442218e27d4119c16a6ae28d5fb7	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	161585545		

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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13290708
Filing Date	2011-11-07
First Named Inventor	EDERY, Yigal
Art Unit	2431
Examiner Name	REVAK, Christopher A
Attorney Docket Number	FIN0001-CON1-CIP1-CON4

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue 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. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	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[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

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[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	1	"Trend Micro's Virus Protection Added to Sun Microsystems Netra Internet Servers," Business Wire, October 1, 1996, available at http://www.cs.indiana. edu/ ~kinzler/pubs/viruswall.html	☐
	2	"Symantec Announces Norton Antivirus 2.0 for Windows NT," Symantec Corporation press release, September 16, 1996, available at http:/ Iwww.symantec.comlabout/news/release/article.jsp?prid= 19960916_01	☐
	3	"Dark Avenger Mutation Engine No Threat to Protected PCs," McAfee, Inc. press elease, May 11, 1992, available at http://securitydigest.org/virus/mirror/www.phreak.orgvirus 1/1992/vinl05.191	☐
	4	"Dark Avenger Mutation Engine No Threat to Protected PCs," McAfee, Inc. press elease, May 11, 1992, available at http://securitydigest.org/virus/mirror/www.phreak.orgvirus 1/1992/vinl05.191	☐
	5	Gryaznov, D.O., "Scanners ofthe Year 2000: Heuristics," Proceedings ofthe Fifth International Virus Bulletin Conference, pp. 225-234 (1995), available at http://vxheavens.comllib/adgOO.html	☐
	6	"Symantec Announces Norton Internet Email Gateway at Internet World - Booth # 369 on December 11, 12, and 13," Symantec Corporation press release, December 11, 1996, available at http:/ Iwww.symantec .comlabout/news/release/article.jsp?prid= 19961211_03	☐
	7	"Internet Security Gets Less Costly and Easier to Manage: Integralis Announces MIMEsweeper Compatible with Check Point Firewall-Ion Single NT Server; E-mail Virus Detection and Content Management Can Reside on Firewall Server, Saving Money and Support Costs," Business Wire, September 16, 1996, available at http://www.thefreelibrary.comlInternet+Security+Gets+Less+Costly+and	☐
	8	"Presenting Java," by John December (1995)	☐
	9	"The Java Language Specification" by Gosling, et al. (1996)	☐
	10	"The Java Programming Language," by Ken Arnold and James Gosling (1996)	☐
	11	"The Java Virtual Machine Specification," by Tim Lindholm and Frank Yellin (1997)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	12	"Computer Viruses and Artificial Intelligence," by David Stang (September, 1995)	☐
	13	"Java Security and a Firewall Extension for Authenticity Control of Java Applets," by Magnus Johansson (January 29,1997)	☐
	14	"Static Analysis of Programs With Application to Malicious Code Detection," by Raymond Lo (1992)	☐
	15	File History for U.S. Patent No. 6,804,780	☐
	16	"Virus Detection Alternatives," by Patrick Min (July, 1992)	☐
	17	"Dynamic Detection and Classification of Computer Viruses Using General Behaviour Patterns," by LeCharlier, et al. (September, 1995)	☐
	18	The Giant Black Book of Computer Viruses by Mark Ludwig (1995)	☐
	19	HotJava: The Security Story	☐
	20	The Java Filter	☐
	21	"A Java Filter," by Balfanz, et al.	☐
	22	"Improved JavaScript and Java Screening Function," by Claunch (May 4, 1996)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	23	"New Version of Java, JavaScript, ActiveX Screening," by Claunch (July 3, 1996)	☐
	24	"A Toolkit and Methods for Internet Firewalls," by Ranum, et al.	☐
	25	"Identifying and Controlling Undesirable Program Behaviors," by Maria King	☐
	26	"PACL's: An Access Control List Approach to Anti-Viral Security," by Wichers, et al.	☐
	27	ENDRIJONAS, Janet, Rx PC The Anti-Virus Handbook. Published in the U.S. in 1993 by TAB Books, a division of McGraw-Hili, Inc. (201 paQes)	☐
	28	"Secure Code Distribution," by X. Nick Zhang (June, 1997)	☐
	29	IBM AntiVirus User's Guide (November 15, 1995)	☐
	30	"Breadth of Runtime Environments and Security Make Java a Good Choice for the Internet" (1996)	☐
	31	Omura, Jim K., "Novel Applications of Cryptography in Digital Communications," IEEE Communications Magazine, pp. 21-29, May, 1990	☐
	32	Okamoto, E., et al., "ID-Based Authentication System For Computer Virus Detection," IEEE/IEE Electronic Library online, Electronics Letters, Vol. 26, Issue 15, ISSN 0013-5194, July 19,1990, Abstract and pages 1169-1170, URL: http://iel.ihs.com:80/cgibinliel_cgi?se ... 2ehts%26ViewTemplate%3ddocview%5fb%2ehts	☐
	33	IBM AntiVirus User's Guide Version 2.4, International Business Machines Corporation, pp. 6-7, November 15, 1995	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	34	Leach, Norvin, et al., "IE 3.0 Applets Will Earn Certification," PC Week, Vol. 13, No. 29,2 pp., July 22, 1996	☐
	35	"Finjan Software Releases SurfinBoard, Industry's First JAVA Security product For the World Wide Web," Article published on the Internet by Finjan Software Ltd., 1 p., July 29, 1996	☐
	36	"Powerful PC Security for the New World of JAVATM and Downloadables, Surfin Shield™," Article published on the Internet by Finjan Software Ltd., 2 pp. 1996	☐
	37	Microsoft® Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet," Microsoft Corporation, including Abstract, Contents, Introduction, and pp. 1-10, October, 1996	☐
	38	Finjan Announces a Personal Java™ Firewall for Web Browsers - the SurfinShield™ 1.6 (formerly known as SurfinBoard)," Press Release of Finjan Releases SurfinShield 1.6, 2 pp., October 21, 1996	☐
	39	Company Profile, "Finjan-Safe Surfing. The Java Security Solutions Provider," Article published on the Internet by Finjan Software Ltd., 3 pp., October 31,1996	☐
	40	"Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0," Las Vegas Convention Center/Pavilion 5 P5551, 3 pp., November 18, 1996	☐
	41	"Java Security: Issues & Solutions," Article published on the Internet by Finjan Software Ltd., 8 pp., 1996	☐
	42	"Products," Article published on the Internet, 7 pp.	☐
	43	Mark LaDue, "Online Business Consultant: Java Security: Whose Business Is It?," Article published on the Internet, Home Page Press, Inc., 4 pp., 1996	☐
	44	Web Page Article, "Frequently Asked Questions About Authenticode," Microsoft Corporation, last updated February 17, 1997, printed December 23, 1998, URL: http://www.microsoft.com/workshop/security/authcodee/signfaq.asp#9, pp. 1-13	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	45	Zhang, X.N., "Secure Code Distribution," IEEE/IEE Electronic Library online, Computer Vol. 30, Issue 6, pp. 76-79, June, 1997	☐
	46	Binstock, Andrew, "Multithreading, Hyper-Threading, Multiprocessing: Now, What's the Difference?," httn:!hlv'\v\v-inteLcom!cd/ids!dcvdoQcr!asmo-na/enfl/20456.htm, Pacific Data Works, LLC, downloaded 7/7/2008, 7 pp.	☐
	47	VirexPC Version 2.0 or later from Microcom	☐
	48	AntiVirus Kit From 1 stAide Software	☐
	49	FluShot+ Series of Products by Ross Greenberg	☐
	50	Symantec Antivirus ofthe Mac version 3.0 or later	☐

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.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] 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	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

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.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

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	/Dawn-Marie Bey/	Date (YYYY-MM-DD)	2013-05-07
Name/Print	Dawn-Marie Bey	Registration Number	44,442

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 record s.

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.

SOPHOS
EXHIBIT 1004 - PAGE 0423

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13290708
Filing Date	2011-11-07
First Named Inventor	EDERY, Yigal
Art Unit	2431
Examiner Name	REVAK, Christopher A
Attorney Docket Number	FIN0001-CON1-CIP1-CON4

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue 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. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	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[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

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[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	1	"Synthesizing Fast Intrusion Prevention/Detection Systems From High-Level Specifications," by Sekar, et al. (1999)	☐
	2	Art of Computer Virus Research and Defense b Peter Szor (February, 2005)	☐
	3	"Process Execution Controls as a Mechanism to Ensure Consistency," by Eugen Bacic (1990)	☐
	4	"Process Execution Controls: Revisited," by Bacic (1990)	☐
	5	"A Flexible Access Control Service for Java Mobile Code," by Corradi, et al. (2000)	☐
	6	"Java Security: Issues & Solutions" (1996)	☐
	7	"Microsoft Authenticode analyzed," by Rohit Khare (July 22, 1996)	☐
	8	"Java Security: Whose Business Is It?" by Mark LaDue (1996)	☐
	9	Microsoft Authenticode Technology (October, 1996)	☐
	10	"Mobile Code Security," by Rubin, et al.	☐
	11	"Protecting Data From Malicious Software," by Schmid, et al.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	12	"Security in the Large: Is Java's Sandbox Scalable?" by Zhong, et al. (April, 1998)	☐
	13	"A Domain and type Enforcement UNIX Prototype," by Badger, et al. (June, 1995)	☐
	14	"Heuristic Anti-Virus Technology," by Frans Veldman	☐
	15	"Standards for Security in Open Systems," by Warwick Ford (1989)	☐
	16	"Secure File Transfer Over TCP/IP," by Brown, et al. (November, 1992)	☐
	17	"Standards in Commercial Security," by Nick Pope	☐
	18	"X.400 Security Features," by Tony Whyman	☐
	19	"Using CASE Tools to Improve the Security of Applications Systems," by Hosmer, et al. (1988)	☐
	20	"Miro: Visual Specification of Security," by Heydon, et al. (October, 1990)	☐
	21	"An Evaluation of Object-Based Programming with Visual Basic," by Dukovic, et al. (1995)	☐
	22	"Visual Basic 5.0 Significantly Improved," by W. Dennis Swift (June, 1997)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	23	"Development of an Object Oriented Framework for Design and Implementation of Database Powered Distributed Web Applications With the DEMETER Project as a Real-Life Example," by Goschka, et al. (1997)	☐
	24	"Detecting Unusual Program Behavior Using the Statistical Component ofthe Nextgeneration Intrusion Detection Expert System (NIDES), by Anderson, et al. (May, 1995)	☐
	25	"A Generic Virus Scanner in C++," by Kumar, et al. (September 17, 1992)	☐
	26	"A Model For Detecting the Existence of Software Corruption in Real Time," by Voas, et al. (1993)	☐
	27	"Protection Against Trojan Horses by Source Code Analysis," by Saito, et al. (March, 1993)	☐
	28	"Information Agents for Automated Browsing," by Dharap, et al. (1996)	☐
	29	"Static Analysis Virus Detection Tools for Unix Systems," by Kerchen, et al. (1990)	☐
	30	"Managing Trust in an Information-Labeling System," by Blaze, et al. (November 4, 1996)	☐
	31	List of Secure Internet Programming Publications from www.cs.printceton.edu	☐
	32	"A Guide to the Selection of Anti-Virus Tools and Techniques," by Polk, et al. (December 2, 1992)	☐
	33	"An Integrated Toolkit for Operating System Security," by Rabin, et al. (August, 1988)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	34	"A Web Navigator With Applets in Caml," by Francois Ronaix (May, 1996)	☐
	35	"Intel Launches Virus Counterattack," by Charles Bruno (August, 1992)	☐
	36	Intel LANProtect Software User's Guide (1992)	☐
	37	"Parents Can Get PC Cruise Control," by George Mannes (July, 1996)	☐
	38	"A New Techniques for Detecting Polymorphic Computer Viruses," by Carey Nachenberg (1995)	☐
	39	"Heuristic Scanners: Artificial Intelligence," by Righard Zwienenberg (September, 1995)	☐
	40	Intel LANProtect, 30-Day Test Drive Version User's Manual	☐
	41	Slade, Robert, "Guide to Computer Viruses: How to A void Them, How to Get Rid of Them, and How to Get Help" (April, 1996)	☐
	42	A Pathology of Computer Viruses by David Ferbranche (November, 1994)	☐
	43	Earl Boebert's post to the greatcircle firewalls mailing list. Taken from http://www.greatcircle.com/lists/firewalls/archive/firewalls.199410 (October, 16, 1994)	☐
	44	CSL Bulletin: Connecting to the Internet: Security Considerations. Taken from http://csrc.nist.gov/publications/nistbul/cs193-07.txt (July 1993)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	45	FAQ: Interscan ViruswalL Taken from http://\veb,archive.org/web/19970605050331/www..antivirus.com/faq/finterscanfaq.html (last updated August 8, 1996)	☐
	46	Network Security and SunScreen SPF-lOO: Technical White Paper, Sun Microsystems, 1995	☐
	47	"Why Do We Need Heuristics?" by Frans Veldman (September, 1995)	☐
	48	"Leading Content Security Vendors Announce Support for Check Point Firewall- 1.3.0; New Partners for Anti-Virus Protection, URL Screening and Java Security," Business Wire, October 7, 1996, available at http://www.allbusiness.comltechnolo gyl computernetworks-computer -networksecurity17274315-1.html#ixzz1gkbKf4g1	☐
	49	"McAfee Introduces Web shield; Industry's First Secure Anti-Virus Solution for Network Firewalls; Border Network Technologies and Secure Computing to Enter into Web Shield OEM Agreements," Business Wire, May 14, 1996, available at http://findarticles.comlp/articles/mi_mOEINlis_1996_ May _14/ai_182834561	☐
	50	"Trend Micro Announces Virus and Security Protection For Microsoft Proxy Server; Also Blocks Java Applets, ActiveX," Business Wire, October 29, 1996, available at http://www.thefreelibrary.comlTrend+Micro+announces+virus+and+security+protection +for+MicrosofL.-aOI8810512	☐

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.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] 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	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

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.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

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	/Dawn-Marie Bey/	Date (YYYY-MM-DD)	2013-05-07
Name/Print	Dawn-Marie Bey	Registration Number	44,442

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 record s.

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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99**)

Application Number	13290708
Filing Date	2011-11-07
First Named Inventor	EDERY, Yigal
Art Unit	2431
Examiner Name	REVAK, Christopher A
Attorney Docket Number	FIN0001-CON1-CIP1-CON4

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue 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. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	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[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

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[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	1	Finjan's Opposition to Websense's Renewed Motion For Judgment as a Matter of Law, dated December 21,2012, filed in Finjan, Inc. v. Symantec Corp., Sophos, Inc., and Websense, Inc., CA. No. 10-cv-593 (OMS)	☐
	2	Declaration of Paul Batcher Re Websense, Inc.s' Proffer of Evidence Re Laches, dated December 19,2012, filed in Finjan, Inc. v. Symantec Corp., Sophos, Inc., and Websense, Inc., CA. No. 10-cv-593 (OMS) (Redacted 12/26/12)	☐
	3	Opposition to Symantec's Motion For JMOL, dated December 17, 2012, filed in Finjan, Inc. v. Symantec Corp., Sophos, Inc., and Websense, Inc., CA. No. 1O-cv-593 (OMS) (Redacted 12/27/12)	☐
	4	Omura, Jim K., "Novel Applications of Cryptography in Digital Communications," IEEE Communications Magazine, pp. 21-29, May, 1990	☐
	5	Okamoto, E., et al., "ID-Based Authentication System For Computer Virus Detection," IEEEIIEE Electronic Library online, Electronics Letters, Vol. 26, Issue 15, ISSN 0013-5194, July 19,1990, Abstract and pages 1169-1170, URL: http://iel.ihs.com:80/cgibin/iel cgi?se .. .2ehts%26ViewTemplate%3ddocview%5fb%2ehts	☐
	6	IBM AntiVirus User's Ouide Version 2.4, International Business Machines Corporation, pp. 6-7, November 15,1995	☐
	7	Leach, Norvin, et al., "IE 3.0 Applets Will Earn Certification," PC Week, Vol. 13, No. 29, 2 pp., July 22, 1996	☐
	8	"Finjan Software Releases SurfinBoard, Industry's First JAVA Security product For the World Wide Web," Article published on the Internet by Finjan Software Ltd., 1 p., July 29, 1996	☐
	9	"Powerful PC Security for the New World of JAVATM and Downloadables, Surfin Shield™," Article published on the Internet by Finjan Software Ltd., 2 pp. 1996	☐
	10	Microsoft® Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet," Microsoft Corporation, including Abstract, Contents, Introduction, and pp. 1-10, October, 1996	☐
	11	Finjan Announces a Personal Java™ Firewall for Web Browsers - the SurfinShield™ 1.6 (fonnerly known as SurfinBoard)," Press Release of Finjan Releases SurfinShield 1.6,2 pp., October 21, 1996	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	12	Company Profile, "Finjan-Safe Surfing. The Java Security Solutions Provider," Article published on the Internet by Finjan Software Ltd., 3 pp., October 31, 1996	☐
	13	"Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0," Las Vegas Convention Center/Pavilion 5 P5551, 3 pp., November 18, 1996	☐
	14	"Java Security: Issues & Solutions," Article published on the Internet by Finjan Software Ltd., 8 pp., 1996	☐
	15	"Products," Article published on the Internet, 7 pp.	☐
	16	Mark LaDue, "Online Business Consultant: Java Security: Whose Business Is It?," Article published on the Internet, Home Page Press, Inc., 4 pp., 1996	☐
	17	Web Page Article, "Frequently Asked Questions About Authenticode," Microsoft Corporation, last updated February 17, 1997, printed December 23, 1998, URL: http://www.microsoft.com/workshop/security/authcodee/signfaq.asp#9, pp. 1-13	☐
	18	Zhang, X.N., "Secure Code Distribution," IEEE/IEE Electronic Library online, Computer Vol. 30, Issue 6, pp. 76-79, June, 1997	☐
	19	Binstock, Andrew, "Multithreading, Hyper-Threading, Multiprocessing: Now, What's the Difference?," http://www.intel.com/cd/ids/developer/asmo-na/eng/20456.htm, Pacific Data Works, LLC, downloaded 7/7/2008,7 pp.	☐
	20	"Frequently Asked Questions About Authenticode," Microsoft Corporation, updated February 17, 1997	☐
	21	"WWWProxyto Cut Off Java," by Carl Claunch (April 12, 1996)	☐
	22	"Combating Viruses Heuristically," by Frans Veldman (September, 1993)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	23	"MCF: A Malicious Code Filter," by Lo, et al. (May 4, 1994)	☐
	24	Anti-Virus Tools and Techniques for Computer Systems by Polk, et al. (1995)	☐
	25	"Dynamic Detection and Classification of Computer Viruses Using General Behaviour Patterns," by LeCharlier, et al. (July 2, 1995)	☐
	26	"Towards a Testbed for Malicious Code Detection," by Lo, et al. (1991)	☐
	27	"Blocking Java Applets at the Firewall," by Martin, et al.	☐
	28	Virus Detection and Elimination by Rune Skardhamar (1996)	☐
	29	Computer Viruses and Anti-Virus Warfare by Jan Hruska (1992)	☐
	30	"Active Content Security," by Brady, et al. (December 13, 1999)	☐
	31	"Low Level Security in Java," by Frank Yellin	☐
	32	"Email With a Mind ofIts Own: The Safe-Tcl Language for Enabled Mail," by Nathaniel Borenstein	☐
	33	"Mobile Agents: Are They a Good Idea?" by Chess, et al. (December 21, 1994)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	34	"Remote Evaluation," by Stamos, et al. (October, 1990)	☐
	35	"Active Message Processing: Messages as Messengers," by John Vittal (1981)	☐
	36	"Programming Languages for Distributed Computing Systems," by Bal, et al. (September, 1989)	☐
	37	"Scripts and Agents: The New Software High Ground," by John Ousterhout (October 20, 1995)	☐
	38	"The HotJava Browser: A White Paper"	☐
	39	The Java Virtual Machine Specification, Sun Microsystems (August 21, 1995)	☐
	40	"Security of Web Browser Scripting Languages: Vulnerabilities, Attacks and Remedies," by Anupam, et al. (January, 1998)	☐
	41	"ActiveX and Java: The Next Virus Carriers?"	☐
	42	"Gateway Level Corporate Security for the New World of Java and Downloadables" (1996)	☐
	43	"Practical Domain and Type Enforcement for UNIX," by Badger, et al. (1995)	☐
	44	"A Sense of Self for Unix Processes," by Forrest, et al. (1996)	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	45	"Antivirus Scanner Analysis 1995," by Marko Helenius (1995)	☐
	46	"State Transition Analysis: A Rule-Based Intrusion Detection Approach," by Ilgun, et al. (March, 1995)	☐
	47	"Automated Detection of Vulnerabilities in Privileged Programs by Execution Monitoring," by Ko, et al. (1994)	☐
	48	"Execution Monitoring of Security-Critical Programs in Distributed Systems: A Specification-Based Approach," by Ko, et al. (1997)	☐
	49	"Classification and Detection of Computer Intrusions," by Sandeep Kumar (August, 1995)	☐
	50	ThunderBYTE Anti-Virus Utilities User Manual (1995)	☐

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.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] 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	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

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.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

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	/Dawn-Marie Bey/	Date (YYYY-MM-DD)	2013-05-07
Name/Print	Dawn-Marie Bey	Registration Number	44,442

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 record s.

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.

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

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

Application Number	13290708
Filing Date	2011-11-07
First Named Inventor	EDERY, Yigal
Art Unit	2431
Examiner Name	REVAK, Christopher A
Attorney Docket Number	FIN0001-CON1-CIP1-CON4

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8079086		2011-12-13	Edery, et al.	
	2	4562305		1995-12-31	Ji, et al.	
	3	5077677		1991-12-31	Murphy, et al.	
	4	5263147		1993-11-16	Francisco, et al.	
	5	5278901		1994-05-05	Shieh, et al.	
	6	5311591		1994-05-10	Fischer	
	7	5319776		1994-06-07	Rile, et al.	
	8	5359659		1994-10-25	Rosenthal	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	9	5361359		1992-08-31	Tajalli, et al.	
	10	5398196		1995-03-14	Chambers	
	11	5412717		1995-05-02	Fischer	
	12	5414833		1995-05-09	Hershey, et al.	
	13	5440723		1995-08-08	Arnold, et al.	
	14	5452442		1995-09-19	Kephart	
	15	5483649		1996-06-09	Kuznetsov, et al.	
	16	5485409		1996-01-16	Gupta, et al.	
	17	5485575		1996-01-16	Chess, et al.	
	18	5524238		1996-06-04	Miller, et al.	
	19	5579509		1996-11-26	Furtney, et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	20	5606668		1997-02-25	Shwed	
	21	5621889		1997-04-15	Lermuzeaux, et al.	
	22	5623600		1997-04-22	Ji, et al.	
	23	5623601		1997-04-22	Vu	
	24	5638446		1997-06-10	Rubin	
	25	5675711		1997-10-07	Kephart, et al.	
	26	5692047		1997-12-25	McManis	
	27	5692124		1997-11-25	Holden, et al.	
	28	5696822		1997-12-09	Nachenberg	
	29	5720033		1998-02-17	Deo	
	30	5724425		1998-03-03	Chang, et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	31	5740248		1998-04-14	Fieres, et al.	
	32	5740441		1998-04-14	Shaio, et al.	
	33	5761421		1998-06-02	Van Hoff, et al.	
	34	5765030		1998-06-09	Nachenberg, et al.	
	35	5765205		1998-08-09	Breslau, et al.	
	36	5784459		1998-07-21	Devarakonda, et al.	
	37	5796952		1998-08-18	Davis, et al.	
	38	5805829		1998-09-08	Cohen, et al.	
	39	5809230		1998-09-15	Pereira, J. L. A.	
	40	5825877		1998-10-20	Dan, et al.	
	41	5832208		1998-11-03	Chen, et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	42	5832274		1998-11-03	Cutler, et al.	
	43	5850559		1998-12-15	Angelo, et al.	
	44	5854916		1998-12-29	Nachenberg	
	45	5859966		1999-01-12	Hayman, et al.	
	46	5864683		1999-01-26	Boebert, et al.	
	47	5867651		1999-02-02	Dan, et al.	
	48	5878258		1999-03-02	Pizi, et al.	
	49	5881151		1999-03-09	Yamamoto	
	50	5884033		1999-03-16	Duvall, et al.	
	51	5889943		1999-03-30	Ji, et al.	
	52	5892904		1999-04-06	Atkinson, et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	53	5951698		1999-09-14	Chen, et al.	
	54	5956481		1999-09-21	Walsh, et al.	
	55	5958050		1999-09-28	Griffin, et al.	
	56	5960170		1999-09-28	Chen, et al.	
	57	5963742		1999-10-05	Williams	
	58	5964889		1999-10-12	Nachenberg	
	59	5974549		1999-10-26	Golan	
	60	5978484		1999-11-02	Apperson, et al.	
	61	5983348		1999-11-09	Ji	
	62	5987611		1999-11-16	Freund	
	63	6070239		2000-05-30	McManis	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	64	6088801		2000-07-11	Grecsek	
	65	6088803		2000-07-11	Tso, et al.	
	66	6092194		2000-07-01	Touboul	
	67	6125390		2000-09-26	Touboul	
	68	6154844		2000-11-28	Touboul, et al.	
	69	6167520		2000-12-01	Touboul	
	70	6263442		2001-07-17	Mueller, et al.	
	71	6339829		2002-01-15	Beadle, et al.	
	72	6351816		2002-02-26	Mueller, et al.	
	73	6425058		2002-07-23	Arimilli, et al.	
	74	6434668		2002-08-13	Arimilli, et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	75	6434669		2002-08-13	Arimilli, et al.	
	76	6480962		2002-11-12	Touboul	
	77	6487666		2002-11-26	Shanklin, et al.	
	78	6519679		2003-02-11	Devireddy, et al.	
	79	6571338		2003-05-27	Shaio, et al.	
	80	6598033		2003-07-22	Ross, et al.	
	81	6643696		2003-11-04	Davis, et al.	
	82	6732179		2004-05-04	Brown, et al.	
	83	6804780		2004-10-12	Touboul	
	84	6917953		2005-07-12	Simon, et al.	
	85	7058822		2006-06-06	Edery, et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	86	7143444		2006-11-28	Porras, et al.	
	87	7210041		2007-04-24	Gryaznov, et al.	
	88	7308648		2007-12-11	Buchthal, et al.	
	89	7343604		2008-03-11	Grabamik, et al.	
	90	7418731		2008-08-26	Touboul	
	91	7613926		2009-11-03	Edery, et al.	
	92	7647633		2010-01-12	Edery, 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[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20100195909		2010-08-05	Edery, et al.	
	2	20030014662		2003-01-16	Gupta, et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	3	20030074190		2003-04-17	Allison	
	4	20030101358		2003-05-29	Porras, et al.	
	5	20040073811		2004-04-15	Sanin	
	6	20040088425		2004-05-06	Rubinstein, et al.	
	7	20050050338		2005-03-03	Liang, et al.	
	8	20050172338		2005-08-04	Sandu, et al.	
	9	20060031207		2006-02-09	Bjamestam, et al.	
	10	20060048224		2006-03-02	Duncan, et al.	
	11	20080066160		2008-03-13	Becker, et al.	

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[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	1	1021276	EP		2000-07-26	Frank Marusiak		☐
	2	1132796	EP		2001-09-12	University of Louvain		☐
	3	0636977	EP		1994-07-27	Chambers		☐
	4	04/063948	WO		2004-07-29	Vihana, Inc.		☐
	5	08-263447	JP		1996-10-11	Sun Microsyst., Inc.		☐
	6	95/033237	WO		1995-12-07	Schnurer, et al.		☐
	7	95/27249	WO		1995-10-12	Intel Corporation		☐
	8	98/21683	WO		1998-05-22	Touboul		☐

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[5]
	1	Doyle, et al., "Microsoft Press Computer Dictionary," Microsoft Press, 2nd Edition, pp. 137-138,1993	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	2	Schmitt, D.A., ".EXE files, OS-2 style," PC Tech Journal, Vol. 6, No. 11, p. 76(13), November, 1988	☐
	3	International Search Report for Application No. PCT/IB97/01626, dated May 14,1999,2 pp.	☐
	4	Supplementary European Search Report for Application No. EP 97 950351, dated November 17,2004,2 pp.	☐
	5	File History for Canadian Application No. 2,275,771, 84 pp.	☐
	6	File History for European Application No. 97950351.3, 58 pp.	☐
	7	File History for Japanese Application No. 10-522345,48 pp.	☐
	8	Lemay, Laura, et al., "Approach of Java Language, Applet, A WT and Advanced Apparatus," First Edition, 25 pp. (translated), August 20,1996 (CS-NB-1999-00238-001)	☐
	9	Order Construing the Terms of U.S. Patent Nos. 6,092,194; 6,804,780; 7,058, 822; 6,357,010; and 7,185,361,4 pp., December 11,2007	☐
	10	PlaintiffFinjan Software, Ltd. 's Opening Claim Construction Brief, 38 pp., September 7, 2007	☐
	11	Defendant Secure Computing Corporation's Opening Claim Construction Brief, 46 pp., September 7,2007	☐
	12	PlaintiffFinjan Software, Ltd. 's Answering Claim Construction Brief (Public Version), 45 pp., September 28,2007	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	13	Defendant Secure Computing Corporation's Responsive Claim Construction Brief (Public Version), 37 pp., September 28,2007	☐
	14	Secure Computing Corporation's Disclosure of Prior Art Pursuant to 35 U.S.c. § 282, 6 pp., February 1,2008	☐
	15	Stang, David J., "Computer Viruses and Artificial Intelligence," Virus Bulletin Conference, pp. 235-257, September, 1995	☐
	16	Johannsen, Magnus, "Java Security and a Firewall Extension for Authenticity Control of Java Applets," Thesis Proposal, Computer Science Department, University of Colorado at Colorado Springs, 5 pp., January 29, 1997	☐
	17	Joint Appendix ofIntrinsic and Extrinsic Evidence Regarding Claim Construction Briefing, Volume 1, October 4, 2007	☐
	18	Joint Appendix ofIntrinsic and Extrinsic Evidence Regarding Claim Construction Briefing, Volume 2, October 4, 2007	☐
	19	Final Joint Claim Construction Chart, August 24,2007	☐
	20	Joint Post-Hearing Claim Construction Chart, October 30, 2007	☐
	21	Plaintiffs Trial Brief (Public Version), January 14,2008	☐
	22	Marcionek, David, "A Complete ActiveX Web Control Tutorial," Available at http://www.codeproject.com/KB/COM/CompleteActiveX.aspx (2006)	☐
	23	Docket for Finjan Software Ltd. v. Secure Computing Corporation, et at., U.S. District Court, District of Delaware (Wilmington), Civil Docket No.1 :06-cv-00369-GMS, 52 pp., retrieved on October 24, 2008 from https:llecf.ded.uscourts.gov/cgibinlDktRpt. pl?6532182820 13655-L 567 0-1	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	24	Docket for Finjan Software Ltd. v. Aladdin Knowledge Systems, Inc., et al., U.S. District Court, District of Delaware (Wilmington), Civil Docket No.1 :08-cv-00300-GMS, 5 pp., retrieved on October 24, 2008 from https:llecf.ded.uscourts.gov/cgi-bin-DktRpt.pl?994267838982431-L 567 0-1	☐
	25	Firewall Toolkit (FWTK) 2.0 Beta Release, 1996	☐
	26	International Search Report for Application No. PCT/ILOSI0091S, 2 pp., dated March 3, 2006	☐
	27	Written Opinion for Application No. PCT/ILOSI0091S, S pp., dated March 3,2006 (mailing date)	☐
	28	International Search Report for Application No. PCT/IBOI/01138, 3 pp., September 20, 2002 (mailing date)	☐
	29	International Preliminary Examination Report for Application No. PCT/IBOI/01138, 2 pp., dated December 19, 2002	☐
	30	Gerzic, Amer, "Write Your Own Regular Expression Parser," November 17, 2003, 18 pp., Retrieved from the Internet: http://www.codeguru.com/Cpp/Cpp/cpp_mfc/parsing/article.php/c4093/	☐
	31	Power, James, "Lexical Analysis," 4 pp., May 14,2006, Retrieved from the Internet: http://www.cs.may.ie/~jpower/Courses/compilers/notes/lexical.pdf	☐
	32	Sitaker, Kragen, "Rapid Genetic Evolution of Regular Expressions" [online], The Mial Archive, April 24, 2004 (retrieved on December 7,2004), S pp., Retrieved from the Internet: http://www.mail-archive.com/kragen-tol@canonical.org/msg00097.html	☐
	33	"Lexical Analysis: DF A Minimization & Wrap Up" [online], Fall, 2004 [retrieved on March 2, 200S], 8 pp., Retrieved from the Internet: http://www.owlnet.rice.edu/~comp412/Lectures/L06LexWrapup4.pdf	☐
	34	"Minimization ofDFA" [online], [retrieved on December 7,2004], 7 pp., Retrieved from the Internet: http://www.cs.odu.edu/~toida/nerzic/390teched/regular/fa/min-fa.html	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	35	"Algorithm: NFS -> DFA" [online], Copyright 1999-2001 [retrieved on December 7, 2004],4 pp., Retrieved from the Internet: http://rw4.cs.uni-sb.de/~ganimal/GANIFA/page16_e.htm	☐
	36	"CS 3813: Introduction to Formal Languages and Automata - State Minimization and Other Algorithms for Finite Automata," 3 pp., May 11,2003, Retrieved from the Internet: http://www.cs.msstate.edu/~hansenclasses/3813fall01/slides/06Minimize.pdf	☐
	37	Watson, Bruce W., "Constructing Minimal Acyclic Deterministic Finite Automata," [retrieved on March 20,2005],38 pp., Retrieved from the Internet: http://www.win.tue.nl/~watson/2R870/downloads/madfa_algs.pdf	☐
	38	Chang, Chia-Hsiang, "From Regular Expressions to DFA's Using Compressed NF A's," October, 1992, 112 pp., http://www.cs.nyu.edu/web/Research/Theses/chang_chi-hsiang.pdf	☐
	39	Khare, R., "Microsoft Authenticode Analyzed" [online], July 22, 1996 [retrieved on June 25,2003],2 pp., Retrieved from the Internet: http://www.xent.comlFoRKarchive/smmer96/0338.html	☐
	40	Moritz, R., "Why We Shouldn't Fear Java," Java Report, pp. 51-56, February, 1997	☐
	41	Microsoft, "Microsoft ActiveX Software Development Kit" [online], August 12, 1996 [retrieved on June 25,2003], pp. 1-6, Retrieved from the Internet: activex.adsp.or.jp/inetsdklhelp/overview.htm	☐
	42	D. Grune, et al., "Parsing Techniques: A Practical Guide," John Wiley & Sons, Inc., New York, New York, USA, pp. 1-326,2000	☐
	43	Power, James, "Notes on Formal Language Theory and Parsing," National University of Ireland, pp. 1-40, 1999	☐
	44	Scott, et al., "Abstracting Application-Level Web Security," ACM, pp. 396-407,2002	☐
	45	Non-Final Office Action, dated July 23,2012, for Application Serial No. 13/290,708, 10 pp.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

	46	Amendment and Response to Office Action (Dated July 23,2012) Under 37 C.F.R. 1.111 filed October 23,2012 for Application Serial No. 13/290,708,9 pp.	☐
	47	Final Office Action, dated January 7,2013, for Application Serial No. 13/290,708, 7 pp.	☐
	48	Judgment, dated December 21,2012, filed in Finjan, Inc. v. Symantec Corp., Sophos, Inc., and Websense, Inc., C.A. No. 10-cv-593 (GMS)	☐
	49	Finjan's Opposition to Sophos' Renewed Motion For Judgment as a Matter of Law, dated December 21,2012, filed in Finjan, Inc. v. Symantec Corp., Sophos, Inc., and Websense, Inc., C.A. No. 10-cv-593 (GMS)	☐
	50	Finjan's Opposition to Symantec's Motion For Judgment as a Matter of Law at the Close of Evidence, dated December 21,2012, filed in Finjan, Inc. v. Symantec Corp., Sophos, Inc., and Websense, Inc., CA. No. 10-cv-593 (OMS)	☐

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.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] 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	13290708
	Filing Date	2011-11-07
	First Named Inventor	EDERY, Yigal
	Art Unit	2431
	Examiner Name	REVAK, Christopher A
	Attorney Docket Number	FIN0001-CON1-CIP1-CON4

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.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

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	/Dawn-Marie Bey/	Date (YYYY-MM-DD)	2013-05-07
Name/Print	Dawn-Marie Bey	Registration Number	44,442

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 record s.

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.

SOPHOS
EXHIBIT 1004 - PAGE 0457

Electronic Acknowledgement Receipt

EFS ID:	15717863
Application Number:	13290708
International Application Number:	
Confirmation Number:	4120
Title of Invention:	Malicious Mobile Code Runtime Monitoring System and Methods
First Named Inventor/Applicant Name:	Yigal Mordechai Edery
Customer Number:	74877
Filer:	Dawn-Marie Bey./Amanda Bayliss
Filer Authorized By:	Dawn-Marie Bey.
Attorney Docket Number:	FIN0001-CON1-CIP1-CON4
Receipt Date:	07-MAY-2013
Filing Date:	07-NOV-2011
Time Stamp:	20:09:46
Application Type:	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	Non Patent Literature	39NonPatentLiterature.pdf	106077 364bec5c01ecbbc508dc4eda9ffe860d2654cdd0	no	2

Warnings:	
Information:	

2	Non Patent Literature	40NonPatentLiterature.pdf	423721 ec5c04035dd5758d945f789370188f74af8bf5fb	no	6
Warnings:					
Information:					
3	Non Patent Literature	41NonPatentLiterature.pdf	390716 19afd2ad97da962325678170fb1530428df339f9	no	6
Warnings:					
Information:					
4	Non Patent Literature	42ANonPatentLiterature.pdf	7712244 943a914d0e41f07e879d93b35e66f456e5740a88	no	81
Warnings:					
Information:					
5	Non Patent Literature	42BNonPatentLiterature.pdf	7431431 4383c7ca3d28b3e2548bb34b73cf209514318d41	no	82
Warnings:					
Information:					
6	Non Patent Literature	42CNonPatentLiterature.pdf	8129692 1475452e3ddf4bd5967c4575b24a05a11b0e972e	no	81
Warnings:					
Information:					
7	Non Patent Literature	42DNonPatentLiterature.pdf	9320226 875f977f4e10af07a4ac35b08a0f86caacc0ae57	no	82
Warnings:					
Information:					
8	Non Patent Literature	43NonPatentLiterature.pdf	3525936 55a55e23794a9a091f02befb4fc856b1d3eff71a	no	40
Warnings:					
Information:					
9	Non Patent Literature	44NonPatentLiterature.pdf	1066705 33a9ec49ece592c05468ea05c23b837f8ad3031a	no	14
Warnings:					
Information:					
10	Non Patent Literature	45NonPatentLiterature.pdf	368090 9334b2a5a81e1babc38446adf54362d139dd894f	no	10
Warnings:					
Information:					

11	Non Patent Literature	46NonPatentLiterature.pdf	1506964 2d8630b9c33f80d4699be35cc4b2465e9a6b35f1	no	22
Warnings:					
Information:					
12	Non Patent Literature	47NonPatentLiterature.pdf	822474 b0190930f0c052029ac413bf2abd74b7352723ba	no	15
Warnings:					
Information:					
13	Non Patent Literature	48NonPatentLiterature.pdf	300201 907e63736d820a28a0d01b2362a76b1d4b7b690b	no	10
Warnings:					
Information:					
14	Non Patent Literature	49NonPatentLiterature.pdf	305031 97cedd2e6e1b01699c5d6612f55db2456635b6a8	no	9
Warnings:					
Information:					
15	Non Patent Literature	50NonPatentLiterature.pdf	565071 1bfb8d62b03bb66435f691b634704e0a45a1103c	no	15
Warnings:					
Information:					
16	Non Patent Literature	95001836_Part2.pdf	26404 9273623929eb537b9a88a81939b2b55fafac0281	no	1
Warnings:					
Information:					
17	Non Patent Literature	95001836_Part3.pdf	26404 f51cfa768b5c0f23eb68cb2c7f73f572da2da63e	no	1
Warnings:					
Information:					
18	Non Patent Literature	95001836_Part4.pdf	26404 4157846907837770de8eb0d0a08a2dd0f16b2807	no	1
Warnings:					
Information:					
19	Non Patent Literature	95001836_Part5.pdf	4791795 61c30ef9f2e0cd3db7435523ec3d7b0f289098c1	no	162
Warnings:					
Information:					

20	Non Patent Literature	95001836_Part6.pdf	115643 ddc1e1527cb6195e9691341732537a93e77ba809	no	3
Warnings:					
Information:					
21	Non Patent Literature	95001836_Part7.pdf	123645 fde08366ea6560a3453876dc609d61f960c1280b	no	2
Warnings:					
Information:					
22	Non Patent Literature	95001836_Part8.pdf	83040 2f7f8051238b7d1eea5f1bf618886de4f779839f	no	1
Warnings:					
Information:					
23	Non Patent Literature	95001836_Part9.pdf	89517 62369efb65dbf1b7d2196c201094d7dec29c34b6	no	2
Warnings:					
Information:					
24	Non Patent Literature	95001836_Part10.pdf	614225 5af73b3fa8702e8c6297fe4d589b8536f211f461	no	15
Warnings:					
Information:					
25	Non Patent Literature	95001836_Part11.pdf	99979 06df329f9b775b04cf276af243abe2b4c69f3d8b	no	2
Warnings:					
Information:					
26	Non Patent Literature	95001836_Part12.pdf	180450 ee2ef03c5f7e9cd143495b66ff30c35b7c60246b	no	3
Warnings:					
Information:					
27	Non Patent Literature	95001836_Part13.pdf	149672 3ef68c7e7e5260bce6cfdbe61f1f585c7da60659	no	3
Warnings:					
Information:					
28	Non Patent Literature	95001836_Part14.pdf	375909 af2dbecb15fd81a78aca2155706ddd27aa54d594	no	8
Warnings:					
Information:					

29	Non Patent Literature	95001836_Part15.pdf	389046 1f37530847200371dff683282ac33f60e319214c	no	7
Warnings:					
Information:					
30	Non Patent Literature	95001836_Part16.pdf	278949 fac38a9792726366145fd9ad774f54f5b0324f58	no	4
Warnings:					
Information:					
31	Non Patent Literature	95001836_Part17.pdf	641163 1fe1b6061b30eba2c600886f3f15e71876fd3207	no	13
Warnings:					
Information:					
32	Non Patent Literature	95001836_Part18.pdf	25330849 1a33dae6941353241dd31f9b2789f12d6acc9562	no	269
Warnings:					
Information:					
33	Non Patent Literature	95001836_Part19.pdf	382672 06d85bc5c87b3530f01165bb02ed4549688b900d	no	1
Warnings:					
Information:					
34	Non Patent Literature	95001836_Part20.pdf	382672 d1de70b3194033ab8473522a3757a735d6ec4400	no	1
Warnings:					
Information:					
35	Non Patent Literature	95001836_Part21.pdf	382672 34253a9d07899134daa6ee1a36f4c5f265b5a584	no	1
Warnings:					
Information:					
36	Non Patent Literature	95001836_Part22.pdf	4924902 b3fc1ca04d1b3c5ae23c8b39e5858f7ccce22b8a	no	17
Warnings:					
Information:					
37	Non Patent Literature	95001836_Part23.pdf	1955045 be3e3a4fe478ecc80684178e545abe553b4986d3	no	10
Warnings:					
Information:					

38	Non Patent Literature	95001836_Part24.pdf	5064959 47be035f1f1c4db6dff35a8eb0b31020ff0701ad	no	27
Warnings:					
Information:					
39	Non Patent Literature	95001836_Part25.pdf	1586765 d66d59df7c2bf61b6bfba7d6f27830e3fa9ed548	no	30
Warnings:					
Information:					
40	Non Patent Literature	95001836_Part26.pdf	1982994 786d0edbf746cc97025405123274d0f4e8e26f12	no	22
Warnings:					
Information:					
41	Non Patent Literature	95001836_Part27.pdf	2349108 b48b0e99d8025a01fb45e26f4e3dd82d9149ef42	no	9
Warnings:					
Information:					
42	Non Patent Literature	95001836_Part28.pdf	1638166 ae0e910d8de0f4494f332a14d5b814b0b26ea046	no	11
Warnings:					
Information:					
43	Non Patent Literature	95001836_Part29.pdf	1879599 1572db8219ee93f22c4dfd0c65617a646a3b7732	no	18
Warnings:					
Information:					
44	Non Patent Literature	95001836_Part30.pdf	3871444 767888e0e2f54206797fcdbd514a320b6ebfbaf9	no	11
Warnings:					
Information:					
45	Non Patent Literature	95001836_Part32.pdf	793447 a3a5a82195bf6152b424da69ff206a860eb115a0	no	13
Warnings:					
Information:					
46	Non Patent Literature	95001836_Part33.pdf	867533 d103dad50ff9ceaaaec441fe4523869786ba0681	no	14
Warnings:					
Information:					

47	Non Patent Literature	95001836_Part34.pdf	1519700 96108f044e3b90101c78faeff860e280d44cc57e	no	24
Warnings:					
Information:					
48	Non Patent Literature	95001836_Part35.pdf	13251785 defb6e73a16b538c6e7699d03a4f1445ff126f60	no	213
Warnings:					
Information:					
49	Non Patent Literature	95001836_Part36.pdf	47378 5fb98fc7f7bed37b861ee8eac8d5dc2c4c1cab96	no	1
Warnings:					
Information:					
50	Non Patent Literature	95001836_Part37.pdf	47378 0be678de24d071cb4ef6c93bace89c16a23c5a71	no	1
Warnings:					
Information:					
51	Non Patent Literature	95001836_Part38.pdf	47378 fc7bc6121466b2e8757926c0ae9eafad3f017787	no	1
Warnings:					
Information:					
52	Non Patent Literature	95001836_Part39.pdf	47378 98034d8401f7d083eb1ad2c1e1d05f8aa7b9c577	no	1
Warnings:					
Information:					
53	Non Patent Literature	95001836_Part41.pdf	1170046 adccbe01925a219f0036c3bcb6f41408c1a706ac	no	14
Warnings:					
Information:					
54	Non Patent Literature	95001836_Part42.pdf	387673 8b61d53e184828665200b4b84d8e1b75d18555f5	no	5
Warnings:					
Information:					
55	Non Patent Literature	95001836_Part43.pdf	48567 5ec2bff5fc35827e704b049226eeab2664dd41b6	no	1
Warnings:					
Information:					

56	Non Patent Literature	95001836_Part44.pdf	48567 1a4d980a186cf89a71e97f5fd392a63a93c95af2	no	1
Warnings:					
Information:					
57	Non Patent Literature	95001836_Part45.pdf	48567 9347fc4bb27031146c4fba3b6bf23ec6b9650c13	no	1
Warnings:					
Information:					
58	Non Patent Literature	95001836_Part46.pdf	48567 7d93ef3fb6ab23ea4017c95b8ae8065e164371ba	no	1
Warnings:					
Information:					
59	Non Patent Literature	95001836_Part47.pdf	48567 c1b06592b7b0fc0ad13d874de342985b19a6dfa9	no	1
Warnings:					
Information:					
60	Non Patent Literature	95001836_Part48.pdf	48567 6b97462ef5ace1c112718a94a92d98f49e634835	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	120189769		

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.

US005809230A

United States Patent [19]

Pereira

[11] **Patent Number: 5,809,230**

[45] **Date of Patent: Sep. 15, 1998**

[54] **SYSTEM AND METHOD FOR CONTROLLING ACCESS TO PERSONAL COMPUTER SYSTEM RESOURCES**

[75] Inventor: **J. L. A. Pereira**, Buford, Ga.

[73] Assignee: **McLellan Software International, LLC**, Atlantic, Ga.

[21] Appl. No.: **587,143**

[22] Filed: **Jan. 16, 1996**

[51] **Int. Cl.**[6] **G06F 11/00**

[52] **U.S. Cl.** **395/186**

[58] **Field of Search** 395/186, 187.01, 395/188.01, 183.12, 652; 380/3; 364/286.5

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,931,783	6/1990	Atkinson .	
4,951,249	8/1990	McClung et al. .	
5,012,514	4/1991	Renton .	
5,113,442	5/1992	Moir .	
5,212,729	5/1993	Schafer .	
5,263,158	11/1993	Janis .	
5,265,163	11/1993	Golding et al. .	
5,375,243	12/1994	Parzych et al. .	
5,384,910	1/1995	Torres .	
5,483,649	1/1996	Kvznetsov et al.	395/186
5,537,540	7/1996	Miller et al.	395/183.14
5,564,016	10/1996	Korenshtein	395/186
5,586,301	12/1996	Fisherman et al.	395/186
5,627,967	5/1997	Daverer et al.	395/188
5,628,015	5/1997	Singh	395/186
5,657,470	8/1997	Fisherman et al.	395/480
5,701,477	12/1997	Chejlava, Jr.	395/652

OTHER PUBLICATIONS

Microsystem Software, "Microsystem Software Announces Cyber Patrol Internet Access Management Vtility", Ltp: //www.Microsys.Com/prfilcs/cp795.htm, pp. 1–3, Jul. 1995.

Microsoft Press, "Introducing Microsoft Windows 95", pp. 55–57, copyright 1995.

Franklin Tessler, "Launch Pad 1.0", www.macworld.com, Magazine Review, p. 1 Jan. 1995.

Microsystems Software, "Mycrosystems Software Announces Cyber Patrol I.O for Macintosh and Cyber Patrol 2.0 for Windows", http://www.microsys.com/prfiles/cp895.htm, pp. 1–3, Aug. 1995.

Microsystems Software, "Mycrosystems Software Announces Cyber Patrol Home Edition Basic Internet Filtering for Free", http://www.microsys.com/prfiles/cphe–fre-.htm, pp. 1–2, Oct. 1995.

tritech software, Inc. *Winbolt Ver. 1.0 User's Manual*, 1994–1995.

Kent–Marsh Ltd., *Winshield©User Guide*, 1995.

Apple Computer, Inc. *AtEase 3.0 Owner's Guide*, 1995.

Folder Bolt For Windows User Guide, Kent Marsh Ltd., 1994.

Scua Plus, (product brochure, 4 enclosures), Mach II Software, 1989.

Primary Examiner—Robert W. Beausoliel, Jr.

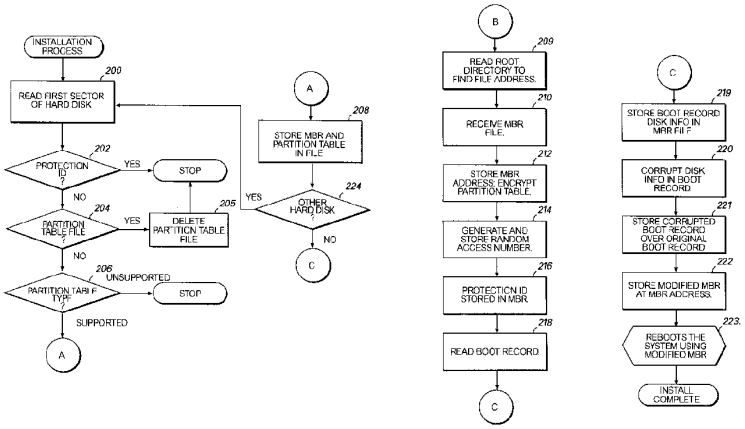
Assistant Examiner—Scott T. Baderman

Attorney, Agent, or Firm—Morris, Manning & Martin, L.L.P.

[57] **ABSTRACT**

A system and method for controlling access to computer resources of a computer is disclosed. The access control program preferably includes a plurality of program components, which may be terminate stay resident (TSR) programs, for intercepting interrupt service calls. The interrupt service calls are verified to determine whether the user is authorized for the resource requested in the service call. The program components use files containing a list of authorized resources for the computer user. These files are, preferably, used at system initialization to modify the system resource files used by the operating system to identify program and program groups which are displayed to a user. A boot protection program is also disclosed which may be installed with the access control program to prevent a boot program stored on media within the diskette drive from acquiring control of the system during system initialization. The boot protection program corrupts the master boot record, boot record and partition table so that other boot programs do not have sufficient information to initialize the system. The master boot program is modified to access this requisite information elsewhere during system initialization.

18 Claims, 10 Drawing Sheets



SOPHOS
EXHIBIT 1004 - PAGE 0466

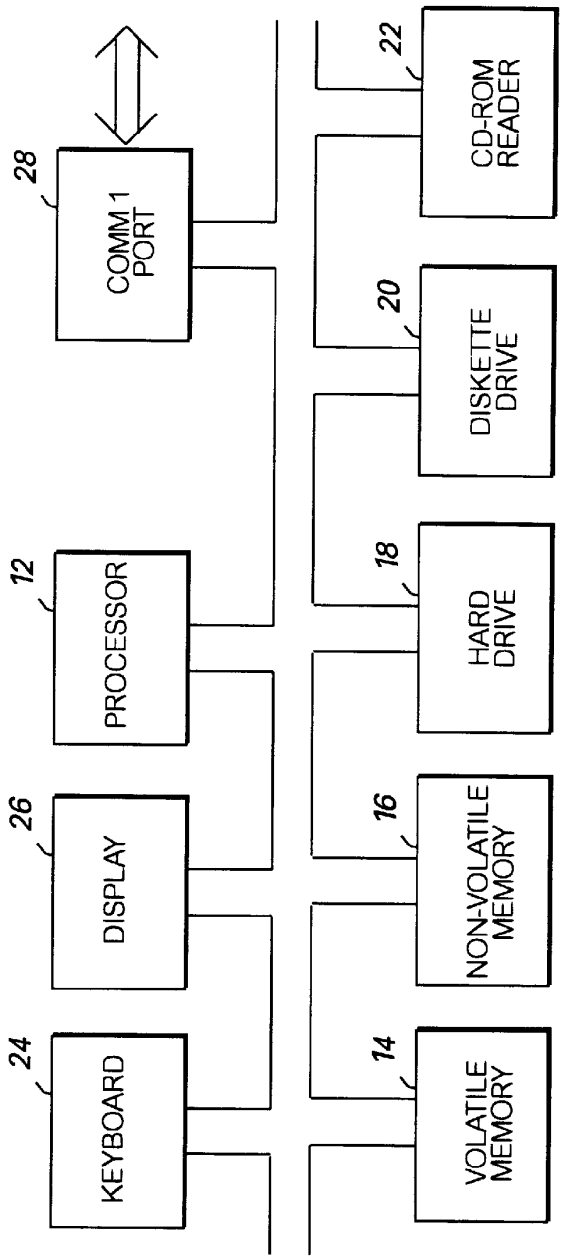

28
COMM 1 PORT
12
PROCESSOR
26
DISPLAY
24
KEYBOARD
22
CD-ROM READER
20
DISKETTE DRIVE
18
HARD DRIVE
16
NON-VOLATILE MEMORY
14
VOLATILE MEMORY

FIG.1

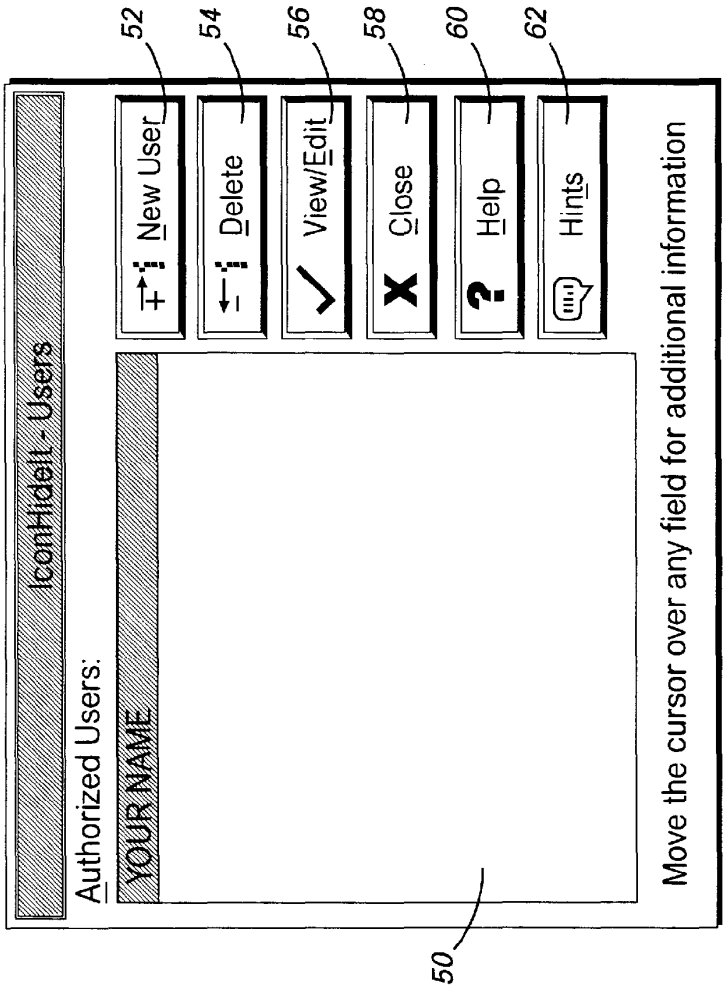

IconHide!t - Users
Authorized Users:
YOUR NAME
New User
Delete
View/Edit
Close
Help
Hints
Move the cursor over any field for additional information
50
52
54
56
58
60
62

FIG. 2

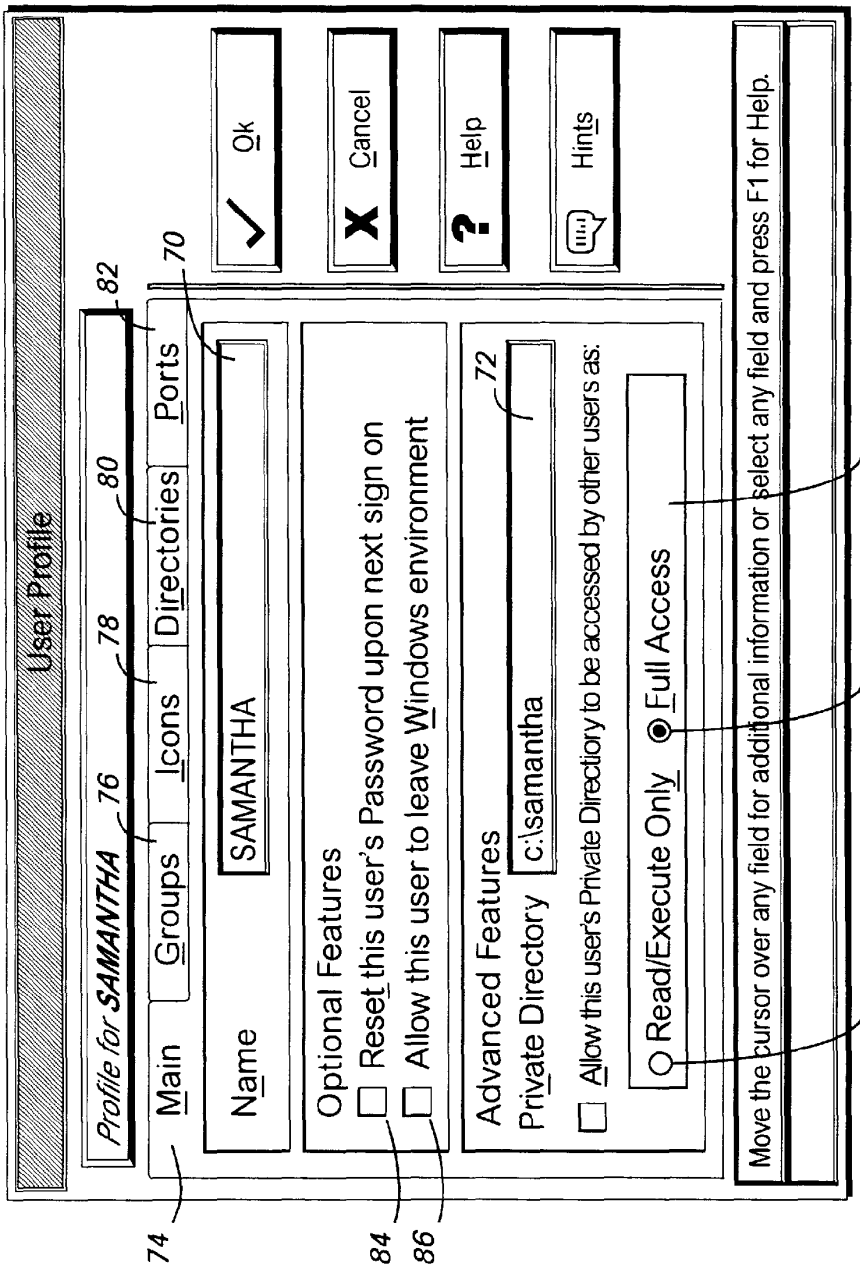

User Profile
Profile for SAMANTHA
Main
Groups
Icons
Directories
Ports
Name
SAMANTHA
Optional Features
Reset this user's Password upon next sign on
Allow this user to leave Windows environment
Advanced Features
Private Directory
c:\samantha
Allow this user's Private Directory to be accessed by other users as:
Read/Execute Only
Full Access
Ok
Cancel
Help
Hints
Move the cursor over any field for additional information or select any field and press F1 for Help.
70
72
74
76
78
80
82
84
86
88
90
92

FIG. 3

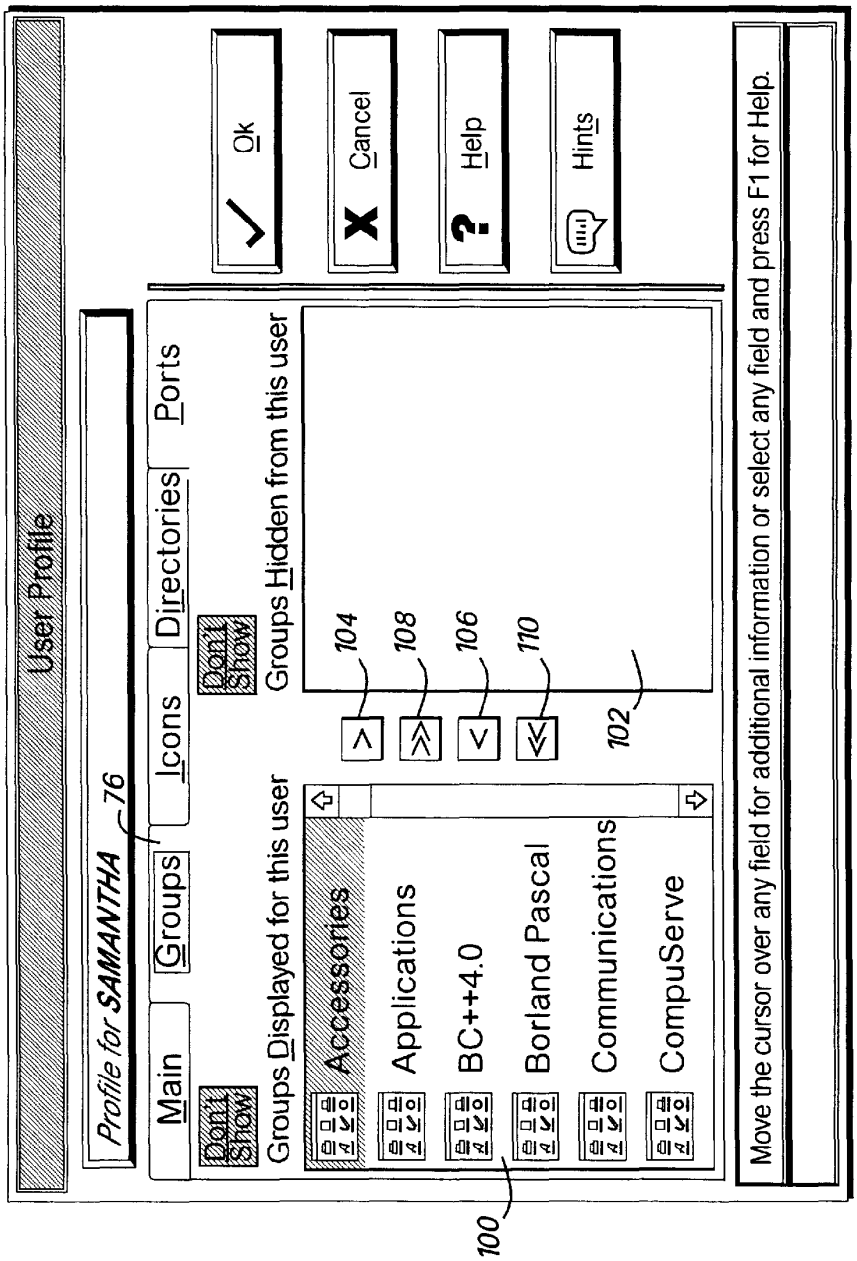

User Profile
Profile for SAMANTHA
76
Main
Groups
Icons
Directories
Ports
Don't Show
Groups Displayed for this user
Accessories
Applications
BC++4.0
Borland Pascal
Communications
CompuServe
Don't Show
Groups Hidden from this user
104
108
106
110
102
Ok
Cancel
Help
Hints
Move the cursor over any field for additional information or select any field and press F1 for Help.
100

FIG.4

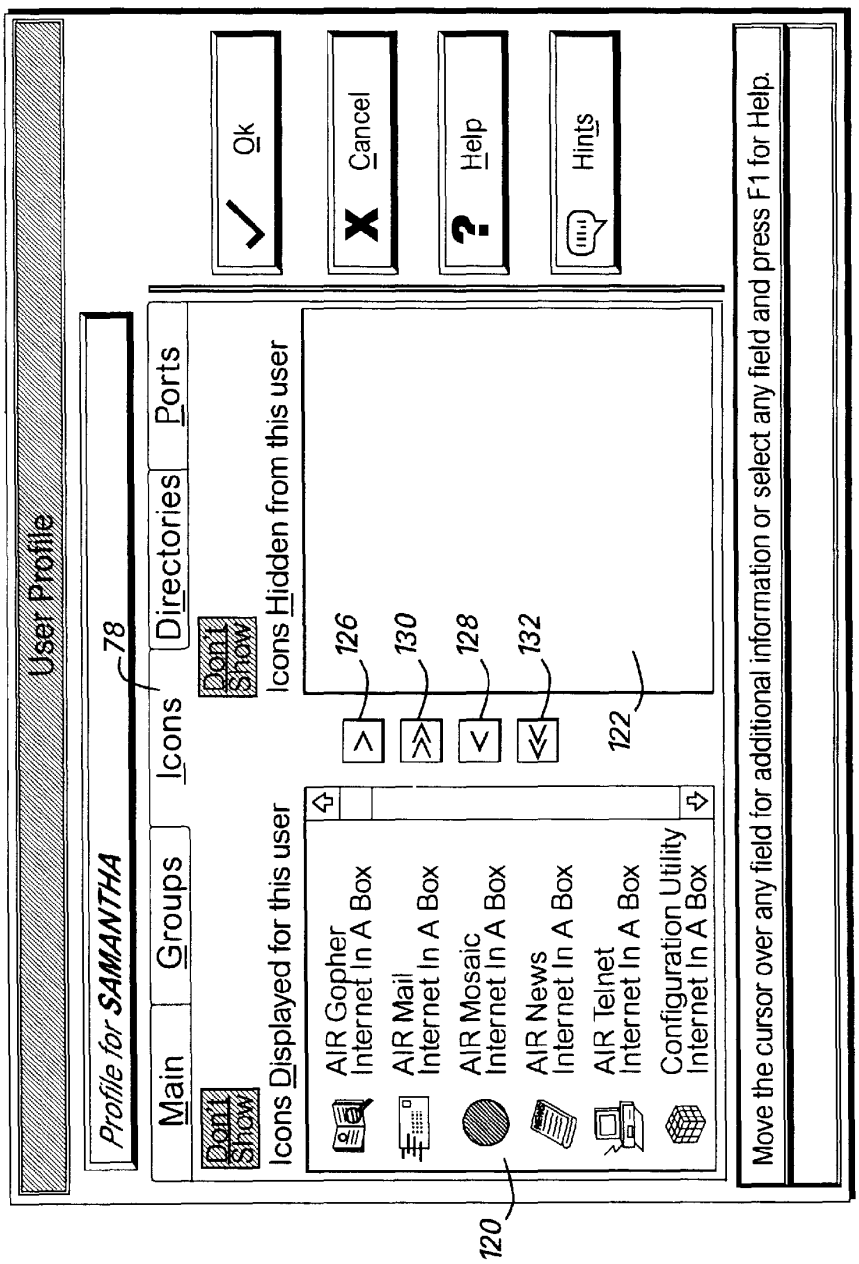

User Profile
Profile for SAMANTHA
78
Main
Groups
Icons
Directories
Ports
Don't Show
Icons Displayed for this user
AIR Gopher Internet In A Box
AIR Mail Internet In A Box
AIR Mosaic Internet In A Box
AIR News Internet In A Box
AIR Telnet Internet In A Box
Configuration Utility Internet In A Box
120
126
130
128
132
122
Don't Show
Icons Hidden from this user
Ok
Cancel
Help
Hints
Move the cursor over any field for additional information or select any field and press F1 for Help.

FIG. 5

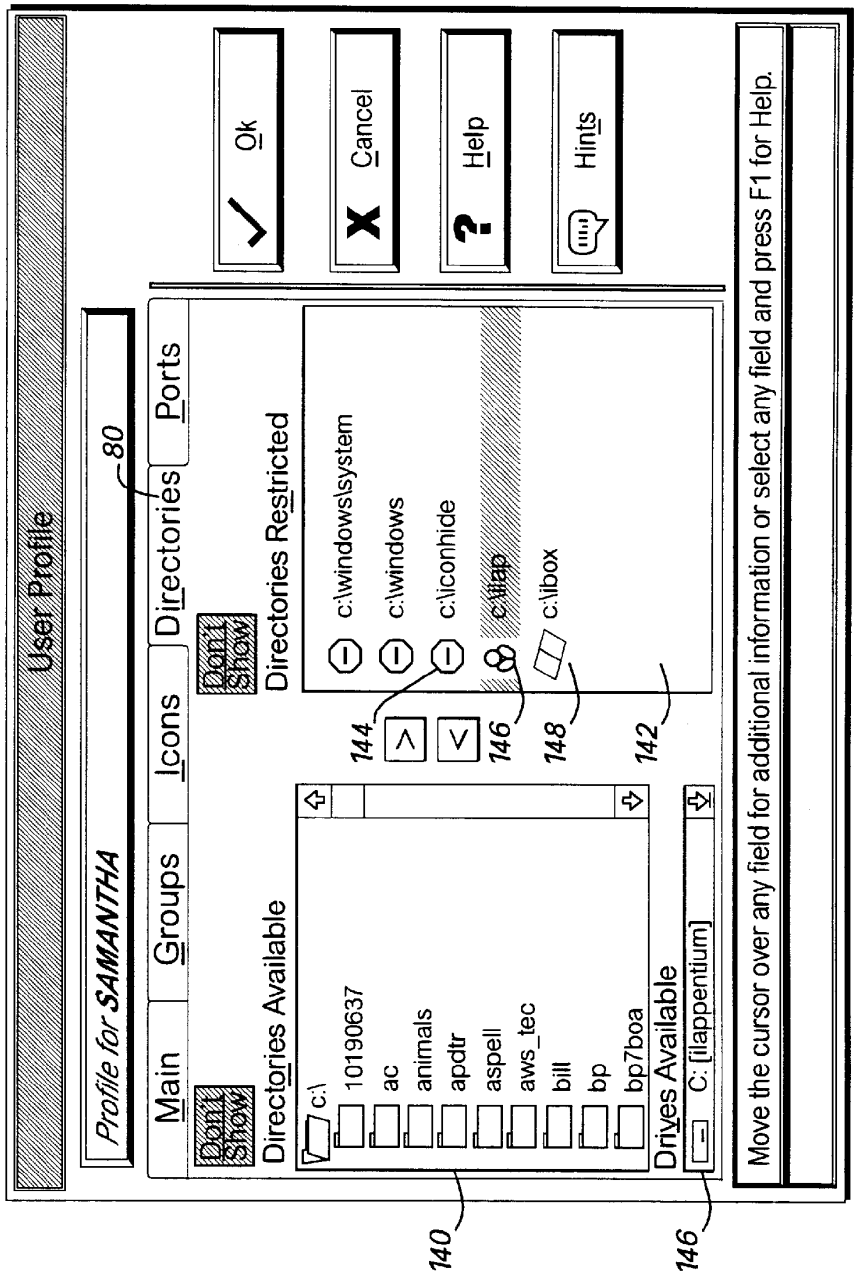

User Profile
Profile for SAMANTHA
80
Main
Groups
Icons
Directories
Ports
Don't Show
Directories Available
c:\
10190637
ac
animals
apdtr
aspell
aws_tec
bill
bp
bp7boa
Drives Available
C: [ilappentium]
Don't Show
Directories Restricted
c:\windows\system
c:\windows
c:\iconhide
c:\lap
c:\ibox
144
146
148
142
140
146
Ok
Cancel
Help
Hints
Move the cursor over any field for additional information or select any field and press F1 for Help.

FIG. 6

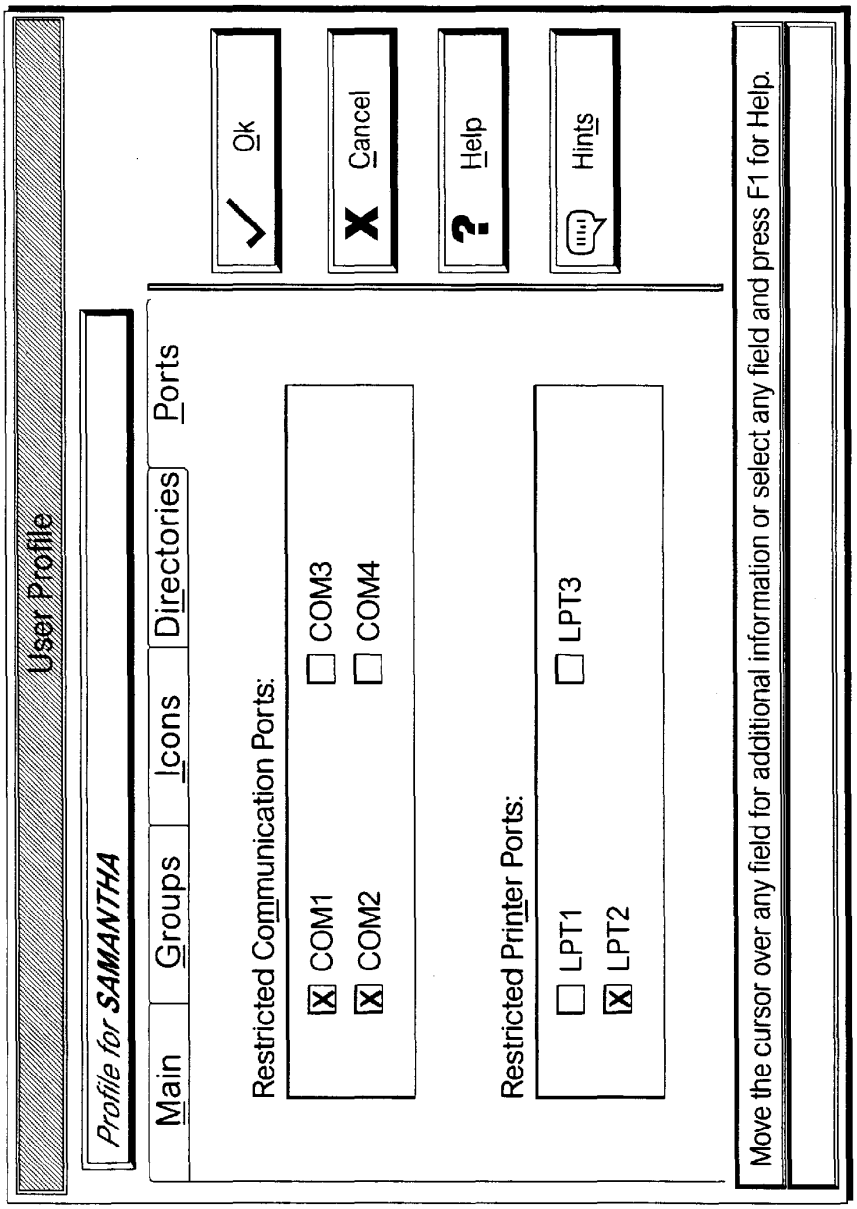

User Profile
Profile for SAMANTHA
Main
Groups
Icons
Directories
Ports
Restricted Communication Ports:
COM1
COM2
COM3
COM4
Restricted Printer Ports:
LPT1
LPT2
LPT3
Ok
Cancel
Help
Hints
Move the cursor over any field for additional information or select any field and press F1 for Help.

FIG.7

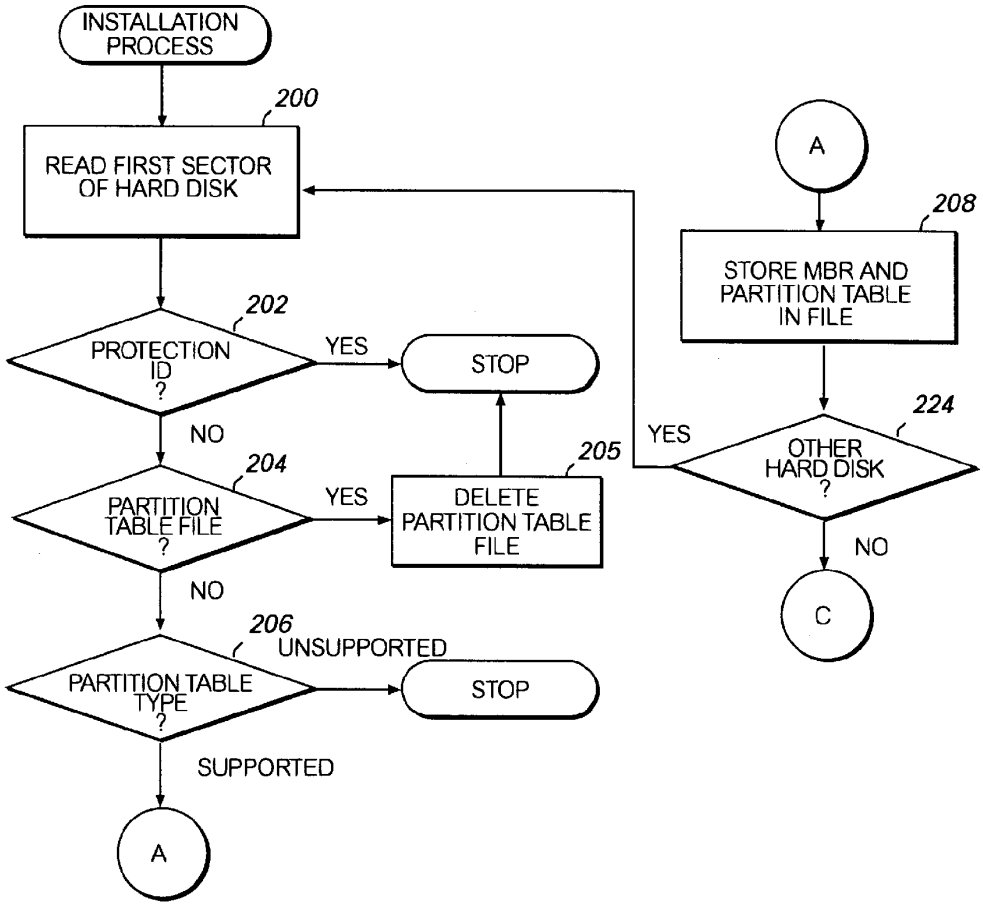

INSTALLATION PROCESS
200
READ FIRST SECTOR OF HARD DISK
202
PROTECTION ID ?
YES
STOP
NO
204
PARTITION TABLE FILE ?
YES
205
DELETE PARTITION TABLE FILE
NO
206
UNSUPPORTED
PARTITION TABLE TYPE ?
STOP
SUPPORTED
A
A
208
STORE MBR AND PARTITION TABLE IN FILE
224
YES
OTHER HARD DISK ?
NO
C

FIG.8A

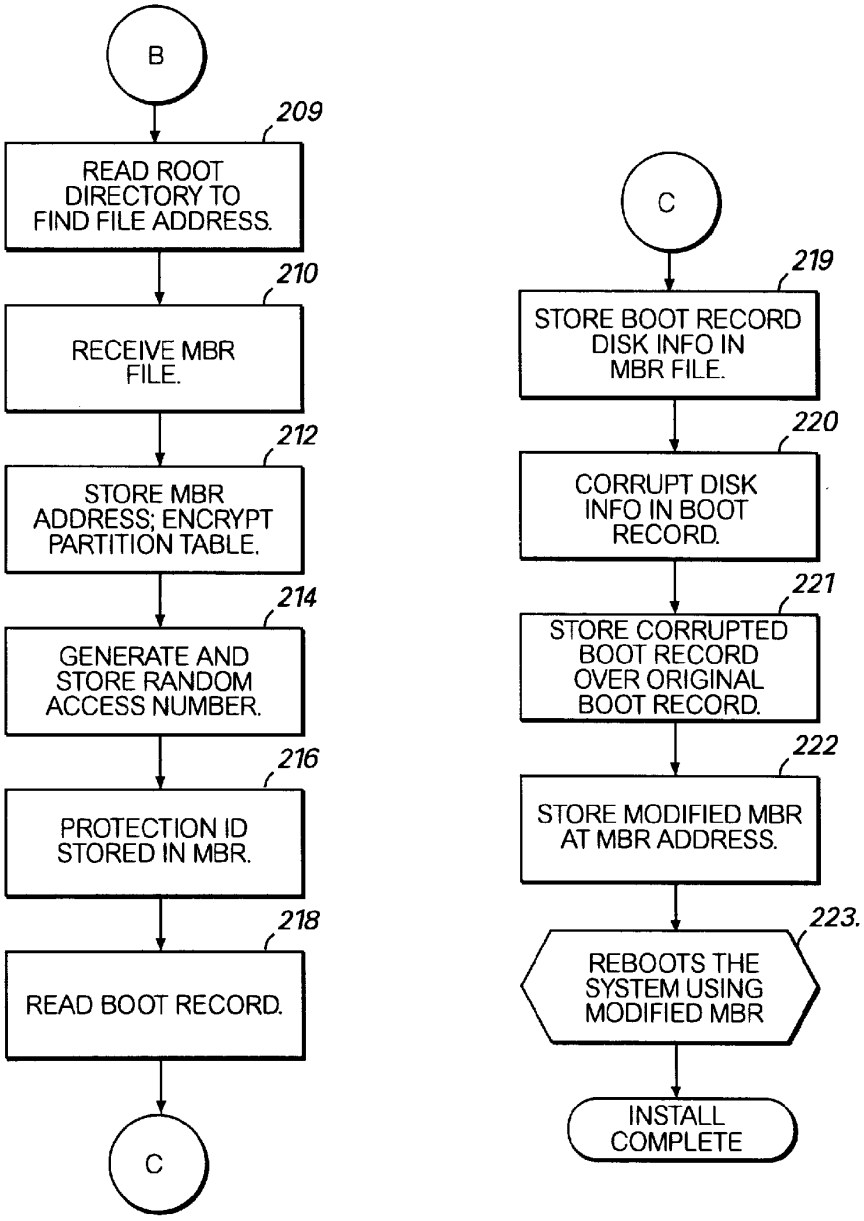

B
209
READ ROOT DIRECTORY TO FIND FILE ADDRESS.
210
RECEIVE MBR FILE.
212
STORE MBR ADDRESS; ENCRYPT PARTITION TABLE.
214
GENERATE AND STORE RANDOM ACCESS NUMBER.
216
PROTECTION ID STORED IN MBR.
218
READ BOOT RECORD.
C
C
219
STORE BOOT RECORD DISK INFO IN MBR FILE.
220
CORRUPT DISK INFO IN BOOT RECORD.
221
STORE CORRUPTED BOOT RECORD OVER ORIGINAL BOOT RECORD.
222
STORE MODIFIED MBR AT MBR ADDRESS.
223.
REBOOTS THE SYSTEM USING MODIFIED MBR
INSTALL COMPLETE

FIG.8B

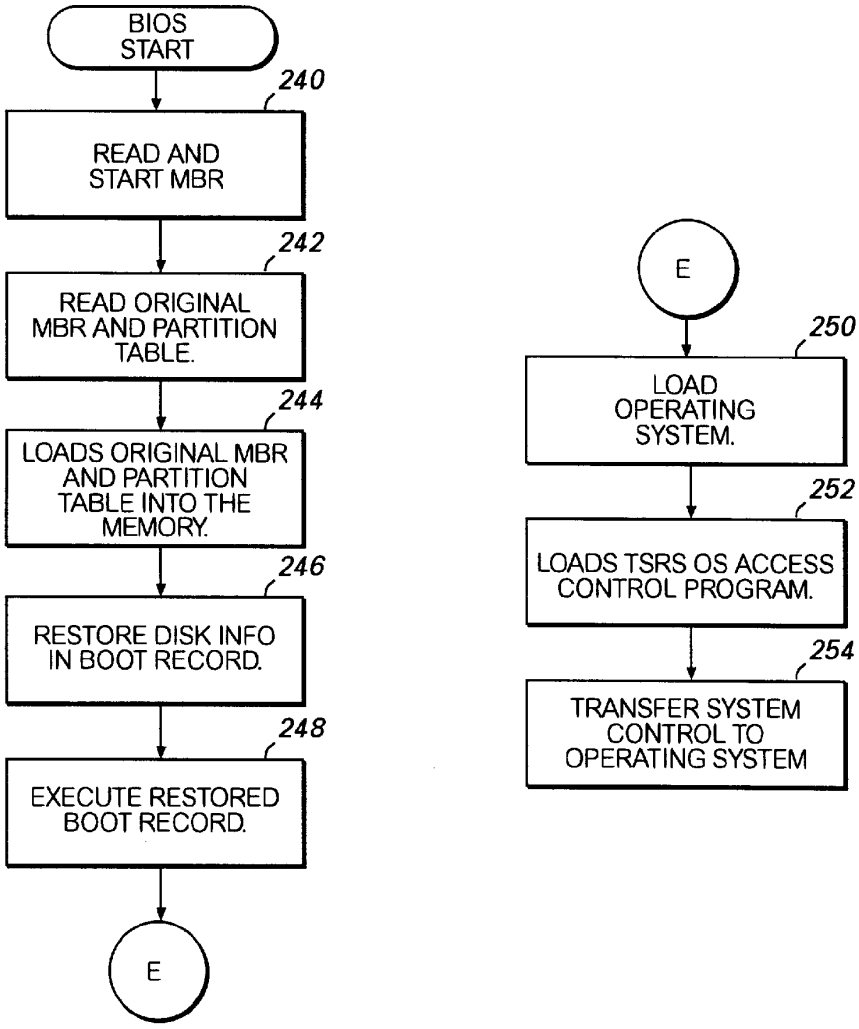

BIOS START
240
READ AND START MBR
242
READ ORIGINAL MBR AND PARTITION TABLE.
244
LOADS ORIGINAL MBR AND PARTITION TABLE INTO THE MEMORY.
246
RESTORE DISK INFO IN BOOT RECORD.
248
EXECUTE RESTORED BOOT RECORD.
E
E
250
LOAD OPERATING SYSTEM.
252
LOADS TSRS OS ACCESS CONTROL PROGRAM.
254
TRANSFER SYSTEM CONTROL TO OPERATING SYSTEM

FIG. 9

SYSTEM AND METHOD FOR CONTROLLING ACCESS TO PERSONAL COMPUTER SYSTEM RESOURCES

FIELD OF THE INVENTION

This invention relates to control of local resources on a personal computer and, more particularly, to control of user authorization and access to local resources on a personal computer.

BACKGROUND OF THE INVENTION

The personal computer, or PC, was first introduced in the early 1980s. These systems generally include a hardware platform of a processor, memory and input/output peripherals that support local resources such as a display monitor, keyboard, hard disk drive, a diskette drive and communication ports. This hardware platform is controlled by an operating system. The operating system is software which controls the interaction between a user and the local resources. Usually this control is performed by controlling the communication interface between utility programs for the local resources and application programs executing on the system.

The number and type of application programs available for a user shortly after the introduction of the PC were not too many or diverse. As a result, the operating system for a PC generally permitted any authorized user to access any resource or file available on the system. However, as PCs proliferated, the number of companies which made software for the systems and the types of software offered for the systems also increased. For example, adult users began to use various financial analysis, organizational, and word processing programs to keep financial records, organize housekeeping or family schedule information and create documents for home and family functions. Adolescents used word processing programs and resource programs such as multimedia encyclopedias to generate reports for school. For younger children, programs for educational interaction or edutainment became commonplace. Thus, all members of a family had a use for the PC and began to need access to the system.

While all family members may have a need for access to the PC, not all members need access to all the resources on a PC. For example, the adults in a family have concerns that the bank records and check balancing files may be inadvertently destroyed by a younger member of the family. Thus, there is a need to segregate files for one user on a PC from the other users. One way to keep a user from accessing certain files is to keep the user from gaining access to the application program that modifies the content of the file. Programs which control access to application programs are known which require a user to enter a password before the operating system activates the program for the user. If the user does not enter the correct password, the requested program is not activated. Without being able to use the program that manipulates the file contents, the user is discouraged from trying to access a particular file.

There are a number of limitations to this protection scheme. For one, all users see all of the application programs that are available on the system. Of course, if a user does not know the password for a program, the user quickly learns that the program is not accessible. For some users this may be satisfactory, however, some inquisitive and talented users may consider the denial of access to a program a challenge. The attempts of such users to circumvent the protection program may result in damage beyond the few files to which

the user was being denied access. Another limitation is that the user may legitimately need access to an application file but not to all of the files which may be manipulated by the application program. For example, an adolescent user may require access to the word processing program to generate a paper for school but not the letter containing details of a personal matter being discussed with a counselor for another member of the family. Programs which use a password to limit access to a file are also known but these programs also notify a user of his or her unauthorized status for the file which may result in attempts to break the access lock. Accordingly, there is a need for denying access to programs or files on a PC without informing the user of the denied access or of the program's or file's existence.

Recently, interest in the Internet and the World Wide Web (WWW) has resulted in millions of PC users purchasing subscriptions to Internet services, browsers for viewing Web sites and high speed modems for downloading files to a PC. While the information services available over the Internet and WWW can be a useful educational supplement to the programs already available on a user's system, there are also sites and services which are not desirable for all members of a family. For example, sexually explicit sites are accessible over the Internet and WWW. Also, some discussion or talk groups may be used by unscrupulous people to contact adolescents or young children so they may later meet the adolescents or children without adult supervision. Thus, there is a need for controlling which users may access the programs and communication resources required for Internet and WWW access.

Granting a user access to certain programs or files should not mean that the user's access rights are unqualified. For example, a parent may wish to deny access to the game programs available on a PC during the afternoon hours for a school age family member but would like to encourage the use of the PC for preparation of the student's work. However, the parent may want to grant access to the games after completion of the student's homework as a reward for a job well done. Currently, a parent would not be able to achieve such time selective control over the programs, files and resources of a PC in an automatic manner.

Some users, who become aware of resources to which they are denied access, attempt to circumvent access control systems and methods by aborting operating system operation and rebooting the system. The user may then attempt a number of methods for obtaining access to the denied resource. One method is to let the reboot proceed until the operating system is loaded but terminate the reboot before the user interface program begins execution. Usually the user interface or some program associated with it performs the access control function. By terminating the reboot prior to the user interface activation, a user knowledgeable about operating system commands may use the operating system to explore the resources available on the system. The user may even by able to modify the access control program to grant the user rights to resources previously denied to the user. Another method of obtaining unauthorized access is to place a system disk containing a system initialization program written by the user in the diskette drive of the system. Most PCs examine the diskette drive for a system initialization program following execution of the Basic Input and Output System (BIOS) program. The BIOS program is a low level program that initializes and verifies basic input and output functions of the PC and then relinquishes control for the remainder of system initialization. If the user's system initialization file on the diskette drive is executed before the initialization file on the hard disk is started, then the user

SOPHOS
EXHIBIT 1004 - PAGE 0477

may prevent the user interface and access control program from being executed.

One known way of preventing a system boot from a diskette drive is to install an extended BIOS card and program. Such cards and programs are set forth in U.S. Pat. Nos. 4,951,249 and 5,113,442. These devices modify the interrupt vectors for the hard disk and keyboards so that the new routines executed in response to these interrupts do not permit a user to gain unencumbered access to the operating system or hard drive. While these devices may be effective, they both require an expansion card which must be inserted in the expansion card bus. Thus, these devices take a card slot which may be otherwise used to enhance the performance of the PC. Additionally, such devices may be defeated by powering down the system and simply removing the expansion card. What is needed is a way of preventing a system boot from a diskette drive without adding a hardware component to the system which may be removed to defeat the system.

At the time that PCs were introduced into the market place the Disk Operating System (DOS) was frequently used for the systems. Because many users found DOS commands cryptic or difficult to understand, user interfaces which communicated between a user and DOS were developed. The interface which is installed in many, if not most, of the PCs today is the Windows program interface from Microsoft of Redmond, Washington. The Windows program facilitates a user's interaction with a PC because it permits a user to activate programs by simply placing a cursor over an icon by using a mouse and activating the program by depressing a button on the mouse. Selections within a program are provided by the Windows program in like manner through a Graphical User Interface (GUI). Thus, many PC users view Windows as an operating system, even though it is an interface between GUI and DOS programs. However, some users see Windows as an unsecured access port to a PC. To gain access to the PC, such users abnormally terminate a program or terminate the execution of the Windows program itself, to gain access to DOS. Since these users are familiar with DOS, they may then investigate the PC and its resources without intervention from an access control component of the Windows program. What is needed is an access control program that is seamless across the Windows/DOS interface.

As can be ascertained from the discussion above, there is a need for a PC access control system and method that can limit each user to a predefined set of resources on the PC without informing the user of the resources not available to the user. There is a need for a PC access control system and method that permits time selective control over a PC's resources. There is also a need to prevent a system boot from a program stored on media in the diskette drive of the PC. There is also a need for a PC access control system and method which provides seamless access control over a Windows/DOS interface in a PC.

SUMMARY OF THE INVENTION

The above limitations of previously known PC access control systems are overcome by a system and method implemented in accordance with the principles of the present invention. The method of the present invention includes the steps of storing a user identifier and a list of computer resources for each user of a PC system, displaying only the computer resources in the list corresponding to the user identifier for the user active on the PC system so that the user active on the PC system only sees the resources which the user may access, and limiting said active user's access to the computer resources in the list of computer resources stored with the user identifier.

This inventive method does not indicate to a user on a PC system the other resources on the system which are not accessible by the user. Accordingly, there is a reduced likelihood that the user knows what other resources are on the PC system and this in turn reduces the likelihood that the user will attempt to gain access to the other resources on the system. On PCs implementing a Windows program type interface, the list of the computer resources are preferably kept in files which are used to modify Group and INI files through the Dynamic Data Exchange (DDE). The modified system files are used to display group and program icons which may be activated by a user to launch a program. Once the system files have been modified, the access control program prevents a user from restoring the deleted group displays and programs to the system files. Thus, the user cannot restore deleted group displays and programs even if the user knows the file names for deleted resources. To restore the system files for the next user, the method of the present invention encrypts and stores an unabridged version of the system files which contain all of the groups and programs which are available on the system to a user having no limitations. At the system start-up for each user, the method retrieves and decrypts the unabridged version and deletes those programs and groups not contained in the corresponding list for the user. In this way, the system may be configured to only display the authorized resources for each user without losing a reference to all programs and groups possible on the system.

The method of the present invention is preferably implemented with three program components. One program component maintains a memory map for the address space for which a user is authorized. A second program component monitors all DOS or Windows file management access calls and verifies whether the user is authorized to access a file, directory, drive, or port. A third program component monitors all BIOS functions and verifies whether the requested access is authorized. As a result, system calls which a knowledgeable user may attempt to execute through user written programs, abnormally terminated programs, DOS or Windows system calls, or BIOS functions are trapped by one of the program components. The program components respond with error messages for resources for which the user is not authorized. An additional benefit of this preferred implementation is that each program component verifies the existence of the other two program components whenever one program component is executed. This protects against a user modifying one program component in an effort to circumvent the system. Whenever an uncorrupted program component executes, it would detect the change in the other program components and immediately execute a system reset. The initialization following system reset restores the program components from the hard disk. Most preferably, the program components in the Windows 3.x environment are implemented with terminate stay resident (TSR) programs while virtual device drivers (VxD) programs are used in Windows 95 systems.

The system of the present invention also uses the DOS Protected Mode Interface (DPMI) to restrict access to a user regardless of whether DOS or the Windows interface program is operating. Normally, DOS and Windows programs execute in mutually exclusive address spaces. For that reason, an exit from the Windows operating environment would cause the DOS programs to execute without access to the restricted use lists that had been used in the Windows

SOPHOS
EXHIBIT 1004 - PAGE 0478

environment. However, the program component that implements the operating environment change provides the addresses of the program component memory space to the DPMI of the Intel or Intel equivalent processor. This permits the program components to continue to execute with access to the restricted lists even though the operating environment has changed.

The method of the present invention may be further supplemented by a boot program protection method which prevents a boot program stored on media within a diskette drive from initializing the system. The boot program protection method includes storing the master boot record and partition table of the PC system hard drive in a non-standard location on the hard drive. This means that a system initialization program implementing the method of the present invention knows where to access the master boot record and partition table to initialize the system. To further frustrate a user boot program which may attempt to intervene during system initialization, the method of the present invention removes hard disk size and format data from the boot record and encrypts the partition table at the standard location on the hard disk. At system initialization, the master boot record restores the boot record as it can ascertain the location of files on the hard disk needed for system startup such as CONFIG.SYS and others. This software only protection scheme is more simple to install and more difficult to defeat than the previously known methods which require the addition of an expansion card or the like.

The system of the present invention includes a computer program that resides on the hard disk of the PC system. The program includes a primary user module which is used by the person installing the program to define the programs, files, directories, times of access, and hardware resources which may be accessed by each user. These files each contain a user identifier and list of computer resources defined as being accessible by the user. These files are encrypted and stored at locations on the hard drive only known to the access control program. Since the access control program may also implement the boot program protection method as well, there may be further difficulty in another being able to ascertain the location of the list files on the hard disk. The program also includes a startup module which is activated during system startup once a user has been authorized for system startup. The startup module uses the identifier corresponding to the authorized user and retrieves the corresponding list of computer resources. This list is then used to modify the system files for the user. These modified files are then stored in memory to be accessed by the access control program. Thereafter, only the programs and groups for which the user is authorized are displayed. Further, any system call for a resource or directory is trapped by one of the Program components of the access control program which sends an error message in response to a request for an unauthorized resource.

Thus, the method and system of the present invention provides an access control program for a PC that may be tailored to limit access to programs, files and other resources of the PC differently for each user. Furthermore, the system maintains a list of the authorized resources for each user regardless of whether the Windows interface or DOS system is the active user interface. The invention may also include a boot protection feature which reduces the likelihood that a user may interrupt system initialization and gain unauthorized access to the PC operating system.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a system in which the present invention is implemented;

FIG. **2** is an illustration of an exemplary display of the manage user function;

FIG. **3** is an illustration of an exemplary display of a user profile;

FIG. **4** is an illustration of an exemplary display of a program group access function;

FIG. **5** is an illustration of an exemplary display of a program icon access function;

FIG. **6** is an illustration of an exemplary display of a directory access function;

FIG. **7** is an illustration of an exemplary display of a port access function;

FIG. **8**A and **8**B are flow charts of the process to install a hard disk protection program which operates in accordance with the principles of the present invention to reduce the likelihood that a boot program stored on media in a diskette drive can be used to initialize the system of FIG. **1**; and

FIG. **9** is a flow chart of how the hard disk protection program controls system initialization and transfers control to the access control program.

DETAILED DESCRIPTION

A personal computer or PC system in which the method and system of the present invention is implemented in shown in FIG. **1**. The system **10** includes a processor **12**, volatile memory **14**, non-volatile memory **16**, and I/O peripherals **18**–**28**, all of which are coupled together by a system bus **34**. Some of the I/O peripherals generate interrupts which cause the processor to transfer program control to a predefined location for interrupt processing and eventual transfer to a routine for servicing the peripheral which generated the interrupt. For example, an interrupt generated by a hard disk typically causes the processor to transfer program control to address **21**H. There the environment of the program currently being executed is saved on the system stack behind the address of the next instruction to process in the interrupted program. Control is then transferred to a hard disk service routine which performs the input or output operation which resulted in the interrupt. Thereafter, the environment of the interrupted program is restored, interrupts reenabled and control transferred to the next instruction address previously stored on the stack.

The system **10**, in which the system and method of the present invention is used, is preferably a personal computer (PC) in which the processor **12** is preferably an Intel 80286 or better or equivalent thereof which implements a DOS Protected Mode Interface (DPMI). Additionally, the method of the present system is preferably implemented in the assembler language for processor **12**. The assembled code for the program components used to implement the method, discussed in more detail below, is stored in files which are stored on hard disk **18**. Preferably, these files are read from hard disk **18** at system initialization and loaded into memory for the DOS operating system or Windows interface program. As known in the art, the memory space of the system is divided so the DOS operating system memory space is mutually exclusive of the memory space used by the Windows interface program. Accordingly, the method of the present invention preferably uses the DPMI to make active the memory in which the program components of the present invention are loaded regardless of whether DOS or Windows is executing. Preferably, the program components of the access control program of the present invention are terminate stay resident (TSR) programs in the Window 3.x environment and virtual device drivers (VxD) programs in a Windows 95 system.

SOPHOS
EXHIBIT 1004 - PAGE 0479

At system power up, the processor begins system initialization by transferring control to a program which verifies the operational status of system memory and the basic input and output operations of the system. Such programs are well known and are generally called BIOS programs. Upon completion of the BIOS program, the system may execute BIOS extensions programs which verify certain expansion devices for the system or control may be transferred to a system initialization file on a user's diskette or hard drive. The system initialization file probably continues by verifying that the user bringing up the system is authorized for use of the system. If the user is authorized, installation of the programs necessary for the operating system and the user interface continues. Control is then transferred to the user interface so the user may begin to select programs for execution and use. If the user is not authorized for system use, the system initialization program denies the user access. After a predetermined number of attempts to gain access have failed, the program aborts system initialization.

Preferably, the resource control system and method of the present invention are implemented by an access control program which is installed on the PC once a user is given access to the system. The program is typically provided on a diskette which is placed in the disk drive of a PC system. The diskette is provided with an installation program which creates a directory for the access control program on the user's hard disk drive. The files containing the program components are then copied into this directory. Part of the installation procedure is to insert commands into a system initialization file, such as the AUTOEXEC.BAT file, before the command which activates an operating system or Windows interface program. These commands activate the program components of the access control program before the operating system or Windows interface program is activated at system initialization. After the access control program is installed, the program requests the user to register as the Primary User and to identify a password. This password is used to identify the Primary User at subsequent logins. After installation of the program and registration of the Primary User, only the Primary User may thereafter install software on the PC, upgrade the access control program or uninstall the access program.

Now the Primary User may use the access control program to add users, define the application programs accessible for each user, and restrict the directories, drives, communication ports and printer ports available for the users. Additionally, the Primary User may allow selected users to be able to exit the Windows interface program and operate within the DOS environment.

To identify or add users to the PC, the Primary User selects the manage users program component. This program component causes a display of the Primary User's name and any other users currently on the system. An exemplary display is shown in FIG. **2**. The Primary User may view a list of authorized users in window **50**. To add a user, the primary user activates the new user function which causes the display of FIG. **3** to appear so the primary user can enter the user's name and resource parameters. The display of FIG. **2** also includes function buttons for deleting a user (**54**), viewing or editing a user's profile (**56**), and closing the manage user function (**58**). A help function (**60**) and hint function (**62**) are also provided to facilitate the primary user's use of the function. In response to the closing of the manage users function, the access control program generates a file of authorized user identifiers and, as each user supplies a password, the file is updated with each user's corresponding password. This file is used by the access control program to limit access to the system to authorized users only.

By activating the view/edit function, the Primary User may also then activate a folder corresponding to one of the previously authorized users. Preferably, the folder is opened by highlighting the user's identifier in window **50** and clicking the mouse cursor over the view/edit function. An exemplary folder for a user is shown in FIG. **3**. As shown in FIG. **3**, the folder includes a window for the user's name (**70**) and a private directory (window **72**) for the user, if one has been identified by the Primary User. The folder preferably includes five tabs which identify the authorized resources for a user. These tabs include main (**74**), groups (**76**), icons (**78**), directories (**80**) and ports (**82**). The main tab is used to identify a directory where a user may keep files which are inaccessible to other users. If the Primary User enters a directory within the private directory window **72**, the access control program creates the directory for the user. The Primary User may also indicate whether the user's password is to be reset (window **84**), whether the user shares the private directory with another (window **88**), and whether the user may leave the Window's environment to operate the DOS environment (window **86**). A user must assign a password to his or her user name at the first sign-in following addition of the user's name to the user list otherwise the access control program does not give the user access to the PC system. If the user's directory is going to be shared with other users, the Primary User may specify whether the user's private directory may be only read by others (windows **90**) or whether others may be able to read and modify the contents of files in the user's private directory (windows **92**).

Upon selecting the tab groups **76**, the Primary User is presented with a display of application program groups. An exemplary display of application program groups is shown in FIG. **4**. Any of the application groups shown in the left-hand window **100** entitled Groups Displayed for this user are available to that user. Conversely, program groups shown in the Groups Hidden from this user window **102** are not available to that user. To move a program from one category to the other, the user may use the mouse cursor to highlight a program group and then click on to the right pointing arrow **104** to transfer the selected program group to the Groups Hidden window **102** or the reverse may be achieved by selecting a program group and clicking on the left pointing arrow **106** to transfer the selected program group to the Groups Displayed window **100**. The double arrow buttons **108** and **110** shown in the exemplary display are preferably used to transfer all of the application groups from one window to the other window. In response to defining the program groups to be displayed and hidden, the access control program generates a file identified by the user's identifier which identifies a list of program groups which are not displayed for user selection.

By activating the icons tab **78**, the Primary User is presented with a display of the program icons for the previously selected program group. An exemplary display of program icons is shown in FIG. **5**. Again, the Primary User may transfer programs from the Icons Displayed window **120** to the Icons Hidden window **122** or from the Icons Hidden window **122** to the Icons Displayed window **120** using arrow functions **126**, **128**, **130** and **132** in a manner similar to that discussed above with respect to FIG. **4**. In response to defining the program icons to be displayed and hidden, the access control program generates a file identified by the user's identifier which identifies a list of program icons which are not displayed for user selection.

By activating the directories tab **80**, the directories on the system are displayed. The directories which may be accessed by a user and those which are not accessible by a

SOPHOS
EXHIBIT 1004 - PAGE 0480

user are shown in the display. An exemplary display for this program component is shown in FIG. **6**. Again, directories and subdirectories may be transferred from the Directories Available window **140** to Directories Restricted window **142** by the method described above with respect to the group and icon windows. Certain directories in the Directories Restricted window **142** cannot be made available to a user. These directories are system directories for the operating system or Windows interface program and the access control program (which is identified in FIG. **6** as the C:\CONHIDE directory). Other directories may be made available to a user on a read only basis. While access to the other directories in the restricted list are completely restricted, the status of these directories may be changed by the Primary User. Preferably, a stop sign **144** is used to indicate the directories for which the restricted status cannot be changed, a lock symbol **146** is used to indicate restricted directories which cannot be accessed by a user, and an open book **148** which is used to identify the directories which are available to a user on a read only basis. Preferably, directory identifiers are limited to 255 characters to comport with the restrictions on directory path names imposed by the operating system or Windows interface program. To restrict a user's access to a drive, the drive is selected in the Drives Available window **146** and the root directory for the drive appears in the Directories Available window **140**. The root directory may then be transferred to the Directories Restricted window **142** to make the drive unavailable for the user. In response to defining the directories which may be accessed by a user, the access control program generates a file identified by the user's identifier which identifies a list of directories to which the user is denied access or whose access is limited to read only.

By activating the ports tab **82**, the ports program component generates a list of the communication and printer ports available on the system. An exemplary display is shown in FIG. **7**. Those communication and printer ports which have an "X" in the window next to a port identifier, such as COM1, indicate that those communication and printer ports have been restricted from use for that user. In response to the definition of these ports as being restricted or not, the access control program generates a file identified by the user's identifier of ports to which the user is denied access.

The restricted lists for the groups, programs, directories, and ports are placed in files which are associated with a user's identifier. These files are then used by the access control program to modify system files when a user signs on the system. Specifically, after system initialization has been performed by the BIOS, control is transferred to the access control program. This program prompts the user for a user name and corresponding password. If the password and user name are verified, the files containing the lists of restricted groups, programs, directories, and ports are read by the access control program. The access control program uses the group and program lists to delete references to those files from the system files. In the Windows 3.x environment this is done by passing the lists to the dynamic data exchange (DDE) which causes the program manager to delete the specified resources from the Group and INI files. Thereafter, the only group folders and program icons which are displayed are those which were not deleted at user sign on. The access control program also monitors calls to the DDE and program manager to prevent the restoration of deleted resources to the system files by a user. The directory and port lists are used to generate tables for the program components of the access control program which control the I/O routines that interface with the drives and ports of the PC system. These tables are maintained in memory with the program components and remain active regardless of whether the operating system or Windows interface program is executing since the DPMI is used to make the memory in which the program components are located accessible. When the program components trap a request for a directory or port, the I/O routine of the program component verifies that the requested directory or port is authorized for the user currently on the system.

In the Windows 95 environment, the access control program modifies the registry file since this file is used to define the computer resources which a user can access and which the Windows 95 program accesses to generate displays of program icons and program groups. Because Windows 95 performs its own user login procedure, the transfer from the login procedure to the access program is done differently. The login procedure in Windows 95 assigns the user a default user registry file if the user cannot enter a password that corresponds with a user's identifier or if the user aborts the login procedure. To prevent this default user from gaining control of the system, the access control program modifies the default user profile in the registry file so the default user is not authorized to use any system resources. If the user enters a corresponding password, however, the files identified by the user's identifier are used to define the resources in the registry file. Since Windows 95 uses this file to display program icons and program groups, the system only displays the ones which the Primary User identified for the user through the access control program. The access control program may use an application program interface (API) to modify the registry system file in accordance with the restricted list files generated by the access control program.

The access control program may also include a function for limiting a user's access to a computer resource to a particular time period. This time restriction may be defined for a program group, program, directory, or port. The access time is stored in the corresponding file for the resource and is accessed by a program component at user login. If any resource has a corresponding access time, the program component retrieves the system time maintained by the system time function and compares system time to the access time to determine whether the resource should be displayed as being available for the user. In this way, the Primary User may deny access to a games program group, for example, during afternoon hours when the user should be using the PC to do his or her homework.

Preferably, the access control program is implemented by three program components. One program component is loaded resident in memory to, preferably, allocate memory space for a user and monitor memory access. This program allocates memory for a user and verifies that the attempted memory access is for a memory location in a memory space authorized for the user. The second program component loaded into memory preferably monitors operating system and/or Windows calls to verify whether the requested resource is authorized for access by the user. The third program component preferably monitors BIOS calls to verify whether the requested resource is authorized for access at system startup. This program is used to detect boot programs which a user may try to use to gain control of the system at initialization. Although these functions may be performed by a single program component, three program components are preferably used. Whenever one of the program components is activated for a verification function, it communicates with the other two program components to verify they are still loaded and are operational. Thus, if a

SOPHOS
EXHIBIT 1004 - PAGE 0481

user is able to find and modify one program component to access unauthorized resources, the other two program components detect the change. In response to a detected change, the program component resets the system so that all three program components are reloaded from the hard disk to memory to overwrite the changed program component. The TSR programs preferably used in the Windows 3.x components environment are loaded into system memory at system initialization. The VxD programs used in a Windows 95 system may be dynamically loaded anywhere in memory.

When the user logs off, the system maintains the same tables and system files until another user tries to log on. If the user is verified, the file containing all of the system resources is retrieved from the hidden location on the hard drive. This file is used to restore the system files of the system. The restricted lists for the user are then retrieved and these lists are used to delete group and programs from the system files and to initialize the tables in the same manner previously discussed. Alternatively, a user may log off and power off the system, in which case, the system simply reboots upon the application of power by the next user.

The access control program also includes a program component for preventing a boot program on the diskette drive from controlling the PC. The executable code for this component is stored in a file on the PC hard disk. When the Primary User installs this feature, the access control program modifies and moves the master boot record (MBR) and partition table on the hard disk. It then modifies the boot record so this component operates following the termination of BIOS operation at system power up.

The installation process for this program component is shown in FIG. **8**. That method begins by reading the first sector of the hard disk (Block **200**) to determine whether this program component has been previously installed (Block **202**). Preferably, this is done by determining whether a particular byte or group of bytes within the first sector has a predetermined value. If the component has been installed previously, the installation stops. Otherwise, the installation program verifies whether the file in which the program stores a copy of the partition table already exists (Block **204**). If it does, then the installation program deletes it (Block **205**) and stops. This is done to permit the hard drive protection program to be installed, if the user wants to add it. Otherwise, the hard disk remains unprotected.

If the program determines that the hard disk protection program has not been previously installed or that any vestige of the program remain, it examines the partition table stored on the hard disk (Block **206**) to determine whether the system operating the disk is compatible with the protection program. For example, DOS and Windows partition a hard disk into four partitions while other operating systems partition the disk differently. If the operating system is not supported then the installation terminates. Otherwise, the program copies the MBR and partition table to a file (Block **208**). This process is repeated for any other hard disks for which the user desires to install the protection (Block **224**).

Installation continues by searching the root directory of the hard disk to locate the cylinder/track/sector address of the file in which the MBR and partition table are stored (Block **209**). The file containing the MBR program is then retrieved (Block **210**). The address of the original MBR on the disk is stored for future reference and the original partition table on the disk is encrypted and rewritten to the disk (Block **212**). Using a random number generator, an access number is generated and stored in the MBR program (Block **214**). This is done to identify whether a user attempting to remove the hard disk protection program is authorized to do so. The protection program identifier is written into the MBR program (Block **216**). The boot record is then read from the hard disk (Block **218**) and the hard disk information, such as disk size, sector size, etc., is retrieved from the boot record and stored in the MBR program (Block **219**). The hard disk drive information in the boot record is corrupted (Block **220**) and the boot record rewritten to the hard disk (Block **221**). The MBR program is then written to the address of the original MBR (Block **222**) and the system is re-initialized with the new MBR to install the hard disk protection program (Block **223**).

The boot process performed in response to system start up under control of the modified MBR program is shown in FIG. **9**. After BIOS has completed its initialization with a normal termination, the BIOS reads the MBR program (Block **240**) and begins its execution. The modified MBR program reads the original MBR and partition table from the hard disk (Block **242**) and loads them into memory (Block **244**). The hard disk information in the modified MBR program is then written into the boot record (Block **246**) and the boot record is stored in memory and executed (Block **248**). The operating system is loaded (Block **250**) and the system initialization batch file (AUTOEXEC.BAT in DOS computers) is executed (Block **252**). The execution of this file loads the program components for the access control program into memory. System control is then transferred to the operating system (Block **254**). Thereafter, interrupts to access the hard disk are intercepted by one of the program components which use the modified MBR program and restored partition table and boot record to control access to the hard disk.

After the hard disk protection program and access control program have been installed, the program and the access control program control access to the operating system and computer resources of the system. Upon system initialization, the BIOS executes and, at its termination, activates the hard disk protection program, if installed. This program controls access to system resources during the remainder of system initialization and loads the operating system and program components for the access control program. Control is transferred to the operating system and the program components of the access control program limit user access to the resources identified in restricted lists as set forth above. If a user attempts to boot the system with a boot program stored on media or a diskette drive, the boot program tries to use the hard disk interrupt to look at the master boot record. In this case, the program is unable to gain sufficient information to search the hard disk and load the operating system. If the hard disk protection program is not installed, system initialization continues with the loading of the operating system and the program components of the access control program, however, the protection provided by the hard disk protection program is not available. Control is then transferred to the operating system. Thereafter, the access control program intercepts interrupt service calls and verifies whether the user is authorized to access the requested resource.

While the present invention has been illustrated by a description of preferred and alternative embodiments and processes, and while the preferred and alternative embodiments and processes have been described in considerable detail, it is not the intention of the applicant to restrict or in any way limit the scope of the appended claims to such detail. For example, a file identified by a user identifier may be generated which contains those resources for which a user is authorized to use. This list of resources may be used

SOPHOS
EXHIBIT 1004 - PAGE 0482

to delete any reference to resources in a system file not contained in the file. Such additional advantages and modifications will readily appear to those skilled in the art.

What is claimed is:

1. A method for limiting a user's access to computer resources of a computer system, comprising:

relocating an original master boot record and an original partition table from a first location to a second location on a hard disk;

providing a corrupted master boot record and a corrupted partition table at said first location so that a program using the corrupted master boot record and said corrupted partition table is unable to initialize said system; and

using, via a security protection program, at system initialization said corrupted master boot record and locating via the security protection program, said original master boot record and said original partition table at said second location to initialize said computer system.

2. The method of claim **1** further comprising the step of:

controlling computer initialization using said relocated master boot record and said relocated partition table; and

installing a program component for controlling access to computer resources in a memory of said system prior to allowing a user to access said computer.

3. The method of claim **1** further comprising the step of:

deleting hard disk information from a boot record; and

storing said hard disk information in said corrupted master boot record so that said hard disk information may be restored in said boot record prior to activating said boot record.

4. The method of claim **1** wherein said second memory location is determining from the steps of:

copying the original master boot record to a file during set-up of the security protection program;

searching the root directory of the hard disk to locate a cylinder/track/sector address of the file containing the original master boot record; and

storing the address of the original master boot record for reference by said corrupted master boot record.

5. A software-implemented system for controlling access to a hard disk during a computer system initialization comprising:

a modified master boot record written to a memory location on a hard disk corresponding to location for an original master boot record;

a corrupted partition table written to a memory location on said hard disk corresponding to a location for an original partition table;

an original partition table stored to a location on said hard disk different from said corrupted partition table; and

a corrupted boot record written to a memory location on said hard disk corresponding to a location for an original boot record whereby said modified master boot record accesses previously stored information during system initialization to restore said boot record for system initialization.

6. The system of claim **5** wherein said modified master boot record loads a program component for controlling user access to computer resources before a user is provided access to a computer.

7. The system of claim **5** said modified master boot record including:

a protection program identifier so that installation of said modified master boot record may be verified.

8. The system of claim **5** wherein said corrupted partition table is encrypted.

9. The system of claim **5** wherein said stored disk information is removed from said original boot record.

10. A computer implemented method that prevents unauthorized access to a computer system, comprising the steps of:

moving an original master boot record from its original location to a non-standard location in memory;

creating a modified master boot record by storing a modified partition table in the modified master boot record that has different specifications than the original master boot record, said modified partition table containing specifications that prevents an operating system from booting from a diskette, thereby preventing access to computer system resources;

storing the modified master boot record at the location corresponding to the original location of the original master boot record; and

using said modified master boot record to control access to computer system resources.

11. The method of claim **10** wherein said non-standard memory location is an arbitrary memory location determined by a security protection program.

12. The method of claim **11** wherein said arbitrary location is determining from the steps of:

copying the original master boot record to a file during set-up of the security protection program;

searching the root directory of a hard disk to locate a cylinder/track/sector address of the file containing the original master boot record; and

storing the address of the original master boot record for reference by said modified master boot record.

13. A computer implemented method that protects a computer system from unauthorized access, comprising the steps of:

accessing a boot record of a hard disk;

changing the boot record data in a manner that prevents an unauthorized user from accessing the hard disk; and

storing information that enables the original boot record data to be restored by an access protection program.

14. The method of claim **13** comprising the steps of:

removing disk information from the boot record of the hard disk; and

storing information removed from said boot record in a manner that enables the original boot record data to be restored by the access protection program.

15. The method of claim **14** further comprising the steps of:

moving a master boot record to a non-standard memory location different than the original location for the master boot record;

creating a modified master boot record which is stored at the original location of the master boot record; and

storing information in the modified master boot record that enables the boot record to be restored by a security protection program.

16. The method of claim **15** wherein said non-standard memory location is an arbitrary memory location determined by the security protection program.

17. The method of claim **16** wherein said arbitrary location is determined from the steps of:

copying the master boot record to a file during set-up of the security protection program;

SOPHOS
EXHIBIT 1004 - PAGE 0483

searching the root directory of the hard disk to locate a cylinder/track/sector address of the file containing the master boot record; and

storing the address of the original master boot record for reference by said modified master boot record.

18. The method of claim **17** further comprising the step of corrupting a partition table in a manner that prevents the computer system from booting.

* * * * *

Electronic Acknowledgement Receipt

EFS ID:	15718260
Application Number:	13290708
International Application Number:	
Confirmation Number:	4120
Title of Invention:	Malicious Mobile Code Runtime Monitoring System and Methods
First Named Inventor/Applicant Name:	Yigal Mordechai Edery
Customer Number:	74877
Filer:	Dawn-Marie Bey./Mary Ellen Quigley
Filer Authorized By:	Dawn-Marie Bey.
Attorney Docket Number:	FIN0001-CON1-CIP1-CON4
Receipt Date:	07-MAY-2013
Filing Date:	07-NOV-2011
Time Stamp:	21:43:55
Application Type:	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	Non Patent Literature	95001836_Part45.pdf	2547312 afc4796c832457cada96d5cc52da894e94e402dd	no	16

Warnings:	
Information:	

2	Non Patent Literature	95001836_Part46.pdf	588378 cd40e437556ba7b6d897d07d4c801f5910b3c428	no	9
Warnings:					
Information:					
3	Non Patent Literature	95001836_Part47.pdf	318889 3cdf9b75be86d9d7f31d54b5b008523c42103f7f	no	4
Warnings:					
Information:					
4	Non Patent Literature	95001836_Part48.pdf	231225 59ed6eb587adabeb0ee071c1f9582140eb292b03	no	5
Warnings:					
Information:					
5	Non Patent Literature	95001836_Part49.pdf	178984 e54ad03ce01c166bee4e85839ed1adacbf53663c	no	4
Warnings:					
Information:					
6	Non Patent Literature	95001836_Part50.pdf	92636 963311f3f8525313e87366b106eee4d85e73b945	no	2
Warnings:					
Information:					
7	Non Patent Literature	95001836_Part51.pdf	17328755 6a745653098a1114712d27eff75e50bc46bdb2d7	no	153
Warnings:					
Information:					
8	Non Patent Literature	95001836_Part52.pdf	17319526 2db7de8115ea135f5c58fda44b9258bedb6ce557	no	154
Warnings:					
Information:					
9	Non Patent Literature	95001836_Part53.pdf	16609434 624ee5e0196269a04d3a97a463b3af71d8a11bcc	no	154
Warnings:					
Information:					
10	Non Patent Literature	95001836_Part54.pdf	18722276 db9725ccf274aa470a49aed055703f1de00fd591	no	153
Warnings:					
Information:					

11	Non Patent Literature	95001836_Part55.pdf	300093 129901ae176a46aee4fc73899719c2b91b448757	no	4
Warnings:					
Information:					
12	Non Patent Literature	95001836_Part56.pdf	1101646 9d5b4594739fd57f493ac3e6f08d2bd14323bf70	no	13
Warnings:					
Information:					
13	Non Patent Literature	95001836_Part57.pdf	516244 09c13c68c277255ae0218698ed55a49264570840	no	6
Warnings:					
Information:					
14	Non Patent Literature	95001836_Part58.pdf	2540739 5ad70ca6596b8e26a3ac8c1cd799e5ef470fc510	no	27
Warnings:					
Information:					
15	Non Patent Literature	95001836_Part59.pdf	5033504 4fbcc499e069735f32071a16f8e06f5f90724525	no	86
Warnings:					
Information:					
16	Non Patent Literature	95001836_Part60.pdf	1146600 88d8fd154fc99678c74c0a2fbeeee2f5a7f84bca	no	25
Warnings:					
Information:					
17	Non Patent Literature	95001836_Part61.pdf	585877 ce0c32b3849da52ffd4438ed69e63d209bc44a7f	no	9
Warnings:					
Information:					
18	Non Patent Literature	95001836_Part62.pdf	341006 d3fb36267dc83bcb3484b4e36213860532e6842a	no	6
Warnings:					
Information:					
19	Non Patent Literature	95001836_Part63.pdf	875877 688a55ec2bbb59dabe9348ea0b2957936f247616	no	4
Warnings:					
Information:					

20	Non Patent Literature	95001836_Part64.pdf	1700132 9e6fd0ef89560f0ef05ea1b54b2e975218f81a2a	no	89
Warnings:					
Information:					
21	Non Patent Literature	95001836_Part65.pdf	330134 fd7f4e8018d752d0c61a197c79106470b874a55a	no	3
Warnings:					
Information:					
22	Non Patent Literature	95001836_Part66.pdf	4812657 6fe5dbc5b52cc433c4fd1b29d4b7aad7a0480ad0	no	134
Warnings:					
Information:					
23	Non Patent Literature	95001836_Part67.pdf	730854 0baeefd42d83bfe5a6b0c592f43425d4eb844b9c	no	9
Warnings:					
Information:					
24	Non Patent Literature	95001836_Part68.pdf	971165 4df7b07ede2ada71323ecb6dff7ededfc6e6b771	no	35
Warnings:					
Information:					
25	Non Patent Literature	95001836_Part69.pdf	3703849 6611ebc01db7f17204639d8a6f95669683499d6b	no	7
Warnings:					
Information:					
26	Non Patent Literature	95001836_Part70.pdf	17312184 2de18e65170bd6c8b984779174f228c5a60eb448	no	305
Warnings:					
Information:					
27	Non Patent Literature	95001836_Part71.pdf	304285 eee7743f13fc686062e4b726d12b776385c3e466	no	6
Warnings:					
Information:					
28	Non Patent Literature	95001836_Part72.pdf	124255 cb0c592f092e614277909c9f0e1758c89bd95809	no	2
Warnings:					
Information:					

29	Non Patent Literature	95001836_Part73.pdf	987774 e03aad2803180c41936f9ac934f4cf7c77c53895	no	36
Warnings:					
Information:					
30	Non Patent Literature	95001836_Part74.pdf	256551 7f5616361e24a76bacfeafef77475408f5f2aeb2	no	3
Warnings:					
Information:					
31	Non Patent Literature	95001836_Part75.pdf	358830 d1839375e390a182f70df024e7494d987d14de26	no	3
Warnings:					
Information:					
32	Non Patent Literature	95001836_Part76.pdf	210953 93b1a32ad8d99b463bda18d1d8e44bdc690b3b2b	no	4
Warnings:					
Information:					
33	Non Patent Literature	95001836_Part77.pdf	152984 007cf1e58ddfd5027a756a8774fb26ad18b71cda	no	2
Warnings:					
Information:					
34	Non Patent Literature	95001836_Part78.pdf	207251 0ecab3d56f72a2ac248726acab3fbcbe415b1e49	no	4
Warnings:					
Information:					
35	Non Patent Literature	95001836_Part79.pdf	150875 bbc204c901edee50c867152b1849f6e8cb8f93ab	no	2
Warnings:					
Information:					
36	Non Patent Literature	95001836_Part80.pdf	1362891 326d82a539351da3bea84340822538e3b05b06ca	no	11
Warnings:					
Information:					
37	Non Patent Literature	95001836_Part81.pdf	162511 a93990c3a556bb46a3c061bf3c3da87fa01ba144	no	3
Warnings:					
Information:					

38	Non Patent Literature	95001836_Part82.pdf	281661 8c7ac7e577d0618ed24f4ff4c8b346415e29b852	no	5
Warnings:					
Information:					
39	Non Patent Literature	95001836_Part83.pdf	2426336 bcb7cfc5990122f847bc6023b205e51e7bff6a74	no	34
Warnings:					
Information:					
40	Non Patent Literature	95001836_Part84.pdf	1472114 87450b3c547ecd53f8d168e8b3a0d6c6a54f5f7b	no	19
Warnings:					
Information:					
41	Non Patent Literature	95001836_Part85.pdf	790602 95303dbd91f72e7689f57dd84f2ae014a299818f	no	12
Warnings:					
Information:					
42	Non Patent Literature	95001836_Part86.pdf	1212115 90fd4d51782b1c3c0f8a38e40778e748635d416b	no	19
Warnings:					
Information:					
43	Non Patent Literature	95001836_Part87.pdf	2018409 7d42f6865815252e0a4514678c713fa7a9400218	no	21
Warnings:					
Information:					
44	Non Patent Literature	95001836_Part88.pdf	14069945 4d7f6de11296f569a7b935591691065201e33d4ea	no	201
Warnings:					
Information:					
45	Non Patent Literature	95001836_Part89.pdf	25177711 24f186b40443cad5741b99b7f083dc5a0d963c24	no	380
Warnings:					
Information:					
46	Non Patent Literature	95001836_Part90.pdf	15518874 705c93b48beeea9ef7555fef62871498d3278d7c	no	227
Warnings:					
Information:					

47	Non Patent Literature	95001836_Part91.pdf	13096984 8eb23994ee039726cc2ee4e3c70da2b83a89adf2	no	171
Warnings:					
Information:					
48	Non Patent Literature	95001836_Part92.pdf	21857353 82d7779e3640c47d161137376b4a30a8f8a1aaf	no	246
Warnings:					
Information:					
49	Non Patent Literature	95001836_Part93.pdf	12561981 ceb41284e9f3a2d873a904c92972cd3a57820387	no	161
Warnings:					
Information:					
50	Non Patent Literature	95001836_Part94.pdf	83296 5a722dd05df5013ec725677aa237fbfa28075f76	no	1
Warnings:					
Information:					
51	Non Patent Literature	95001836_Part95.pdf	83296 2a2190867ad06167aa1ab1670656a91d80d408b0	no	1
Warnings:					
Information:					
52	Non Patent Literature	95001836_Part96.pdf	83296 eb6afbe512dfd2084622b9fe3ba7566951db6aeb	no	1
Warnings:					
Information:					
53	Non Patent Literature	95001836_Part97.pdf	83296 2c4353af21cbc5efa45d3a9890e989ba07a20ab1	no	1
Warnings:					
Information:					
54	Non Patent Literature	95001836_Part98.pdf	83296 65a4ee214aa555df6d5270198662009aa483cc03	no	1
Warnings:					
Information:					
55	Non Patent Literature	95001836_Part99.pdf	83296 f29e064c2bc9f625e8b8d31648daf33704ee7ba5	no	1
Warnings:					
Information:					

56	Non Patent Literature	95001836_Part100.pdf	83296 33a2358e364f8560363bb662698382897605432 0	no	1
Warnings:					
Information:					
57	Non Patent Literature	95001836_Part101.pdf	83296 4de3a00e0cb1e77f9d434f47bfc8dbe2c73facff	no	1
Warnings:					
Information:					
58	Non Patent Literature	95001836_Part102.pdf	83296 fc457a67a7ee00afe761c065e67f6f00d1d6ec1f	no	1
Warnings:					
Information:					
59	Non Patent Literature	95001836_Part103.pdf	83296 c85af967f01dc7f0adbffb226576702589111 8b6	no	1
Warnings:					
Information:					
60	Non Patent Literature	95001836_Part104.pdf	21459139 97e35dc2115e1da084c954d9ceaa213a18d72ab3	no	219
Warnings:					
Information:					
		Total Files Size (in bytes):	252995320		

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.

US006804780B1

(12) **United States Patent**
Touboul

(10) **Patent No.: US 6,804,780 B1**
(45) **Date of Patent: *Oct. 12, 2004**

(54) **SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES**

(75) Inventor: **Shlomo Touboul**, Kefar-haim (IL)

(73) Assignee: **Finjan Software, Ltd.**, Netanya (IL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **09/539,667**

(22) Filed: **Mar. 30, 2000**

Related U.S. Application Data

(63) Continuation of application No. 08/964,388, filed on Nov. 6, 1997, now Pat. No. 6,092,194.
(60) Provisional application No. 60/030,639, filed on Nov. 8, 1996.

(51) **Int. Cl.**[7] **H04L 9/00**; G06F 11/30
(52) **U.S. Cl.** **713/181**; 713/201; 713/176; 717/178
(58) **Field of Search** 713/200, 201, 713/176, 181; 709/223, 225, 227, 229; 717/168–178

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,077,677	A	12/1991	Murphy et al.	
5,359,659	A	10/1994	Rosenthal	
5,361,359	A	11/1994	Tajalli et al.	
5,485,409	A	1/1996	Gupta et al.	
5,485,575	A	1/1996	Chess et al.	
5,572,643	A	11/1996	Judson	
5,579,509	A *	11/1996	Furtney et al.	703/27
5,606,668	A	2/1997	Shwed	
5,623,600	A	4/1997	Ji et al.	
5,638,446	A	6/1997	Rubin	
5,692,047	A	11/1997	McManis	
5,692,124	A	11/1997	Holden et al.	
5,720,033	A	2/1998	Deo	
5,724,425	A	3/1998	Chang et al.	
5,740,248	A	4/1998	Fieres et al.	
5,761,421	A	6/1998	van Hoff et al.	

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

EP	1091276 A1 *	4/2001	G06F/1/00
EP	1132796 A1 *	9/2001	G06F/1/00

OTHER PUBLICATIONS

Khare, "Microsoft Authenticode Analyzed" Jul. 22, 1996, xent.com/FoRK-archive/summer96/0338.html, p. 1–2.*

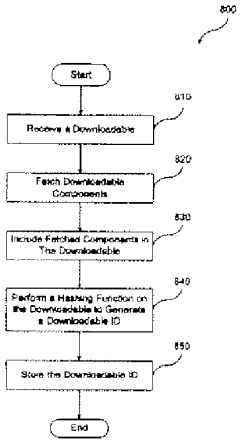
(List continued on next page.)

Primary Examiner—Ayaz Sheikh
Assistant Examiner—Christopher Revak
(74) *Attorney, Agent, or Firm*—Squire, Sanders & Dempsey, L.L.P.

(57) **ABSTRACT**

A computer-based method for generating a Downloadable ID to identify a Downloadable, including obtaining a Downloadable that includes one or more references to software components required by the Downloadable, fetching at least one software component identified by the one or more references, and performing a function on the Downloadable and the fetched software components to generate a Downloadable ID. A system and a computer-readable storage medium are also described and claimed.

18 Claims, 10 Drawing Sheets



U.S. PATENT DOCUMENTS

5,765,205	A		6/1998	Breslau et al.
5,784,459	A		7/1998	Devarakonda et al.
5,796,952	A		8/1998	Davis et al.
5,805,829	A		9/1998	Cohen et al.
5,832,208	A		11/1998	Chen et al.
5,832,274	A	*	11/1998	Cutler et al. 717/171
5,850,559	A		12/1998	Angelo et al.
5,859,966	A		1/1999	Hayman et al.
5,864,683	A		1/1999	Boebert et al.
5,892,904	A		4/1999	Atkinson et al.
5,951,698	A		9/1999	Chen et al.
5,956,481	A		9/1999	Walsh et al.
5,974,549	A		10/1999	Golan
5,978,484	A	*	11/1999	Apperson et al. 705/54
5,983,348	A		11/1999	Ji
6,092,194	A	*	7/2000	Touboul 713/200
6,154,844	A	*	11/2000	Touboul et al. 713/201
6,339,829	B1	*	1/2002	Beadle et al. 713/201

OTHER PUBLICATIONS

"Release Notes for the Microsfot ActiveX Development Kit", Aug. 13, 1996, activex.adsp.or.jp/inetsdk/readme.txt, p. 1–10.*

"Microsoft ActiveX Software Development Kit" Aug. 12, 1996, activex.adsp.or.jp/inetsdk/help/overview.htm, p. 1–6.*

Doyle et al, "Microsoft Press Computer Dictionary" 1993, Microsoft Press, 2nd Edition, p. 137–138.*

Schmitt, ".EXE. files, OS–2 style" Nov. 1988, PC Tech Journal via dialog search, vol. 6, #11, p. 76–78.*

Jim K. Omura, "Novel Applications of Cryptography in Digital Communications", IEEE Communications Magazine, May, 1990; pp. 21–29.

Okamoto, E. et al., "ID–Based Authentication System For Computer Virus Detection", IEEE/IEE Electronic Library online, Electronics Letters, vol. 26, Issue 15, ISSN 0013/5194, Jul. 19, 1990, Abstract and pp. 1169–1170. URL: http://iel.ihs.com:80/cgi–bin/iel_cgi?se . . . 2ehts%26ViewTemplate%3ddocview%5fb%2ehts.

IBM AntiVirus User's Guide Version 2.4, International Business Machines Corporation, Nov. 15, 1995, pp. 6–7.

Norvin Leach et al, "IE 3.0 Applets Will Earn Certification", PC Week, vol. 13, No. 29, Jul. 22, 1996, 2 pages.

"Finjan Software Releases SurfinBoard, Industry's First JAVA Security Product For the World Wide Web", Article published on the Internet by Finjan Softwre Ltd., Jul. 29, 1996, 1 page.

"Powerful PC Security for the New World of Java™ and Downloadables, Surfin Shield™" Article published on the Internet by Finjan Software Ltd., 1996, 2 Pages.

Microsoft® Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet", Microsoft Corporation, Oct. 1996, including Abstract, Contents, Introduction and pp. 1–10.

"Finjan Announces a Personal Java™ Firewall For Web Browsers—the SurfinShield™ 1.6 (formerly known as SurfinBoard)", Press Release of Finjan Releases SurfinShield 1.6, Oct. 21, 1996, 2 pages.

Company Profile "Finjan—Safe Surfing, The Java Security Solutions Provider", Article published on the Internet by Finjan Software Ltd., Oct. 31, 1996, 3 pages.

"Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0" Las Vegas Convention Center/Pavilion 5 P5551, Nov. 18, 1996, 3 pages.

"Java Security: Issues & Solutions" Article published on the Internet by Finjan Software Ltd., 1996, 8 pages.

"Products" Article published on the Internet, 7 pages.

Mark LaDue, "Online Business Consulant: Java Security: Whose Business Is It?" Article published on the Internet, Home Page Press, Inc. 1996, 4 pages.

Web Page Article "Frequently Asked Questions About Authenticode", Microsoft Corporation, last updated Feb. 17, 1997, Printed Dec. 23, 1998. URL: http://www.microsoft.com/workshop/security/authcode/signfaq.asp#9, pp. 1–13.

Zhang, X.N., "Secure Code Distribution", IEEE/IEE Electronic Library online, Computer, vol. 30, Issue 6, Jun., 1997, pp. 76–79.

* cited by examiner

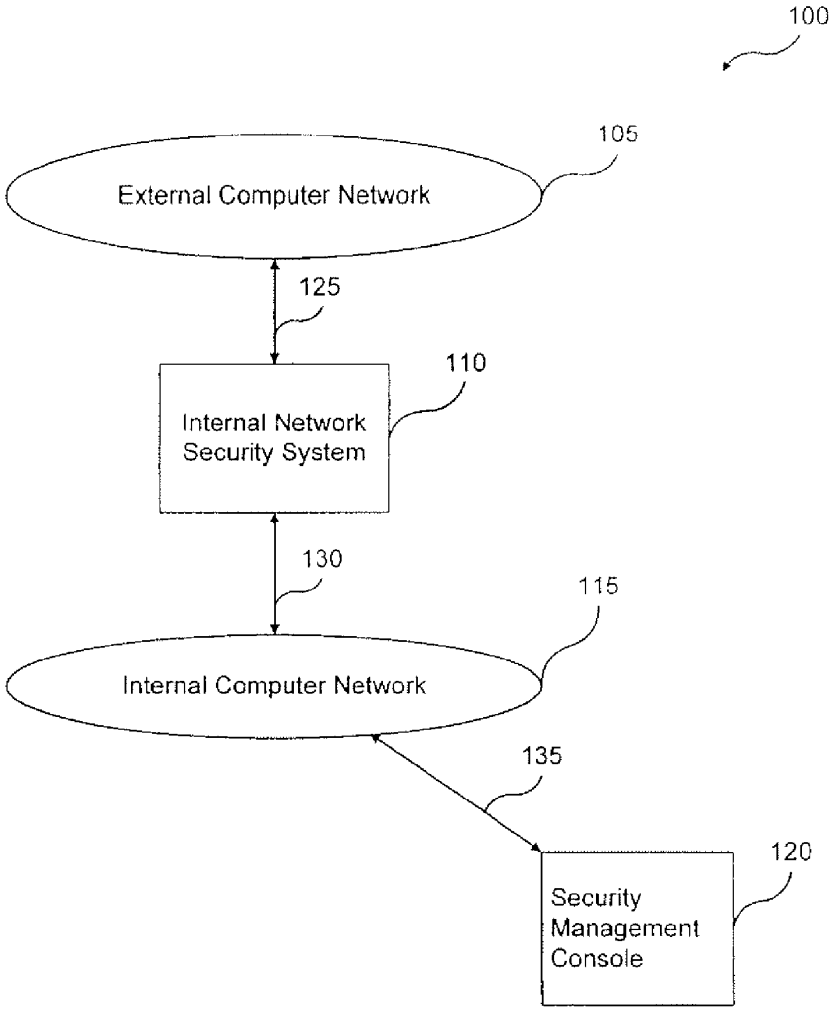

100
105
External Computer Network
125
110
Internal Network Security System
130
115
Internal Computer Network
135
120
Security Management Console

FIG. 1

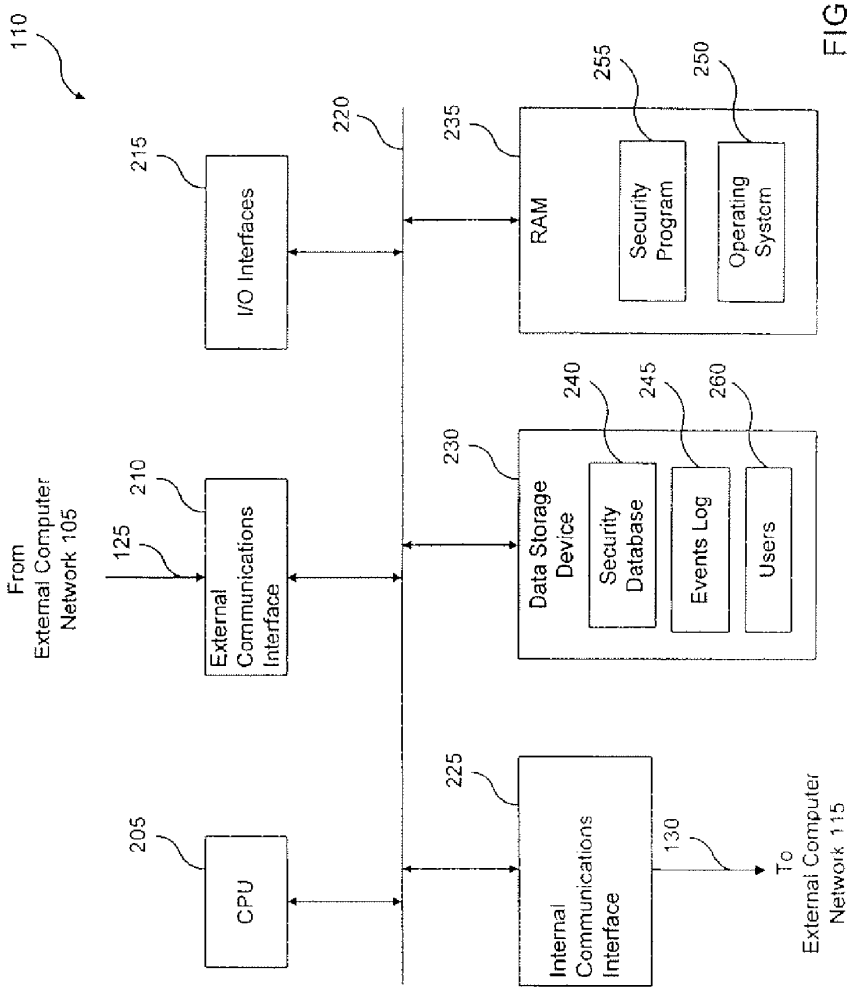

110
215
I/O Interfaces
220
235
RAM
255
Security Program
250
Operating System
From External Computer Network 105
125
210
External Communications Interface
230
Data Storage Device
240
Security Database
245
Events Log
260
Users
205
CPU
225
Internal Communications Interface
130
To External Computer Network 115

FIG. 2

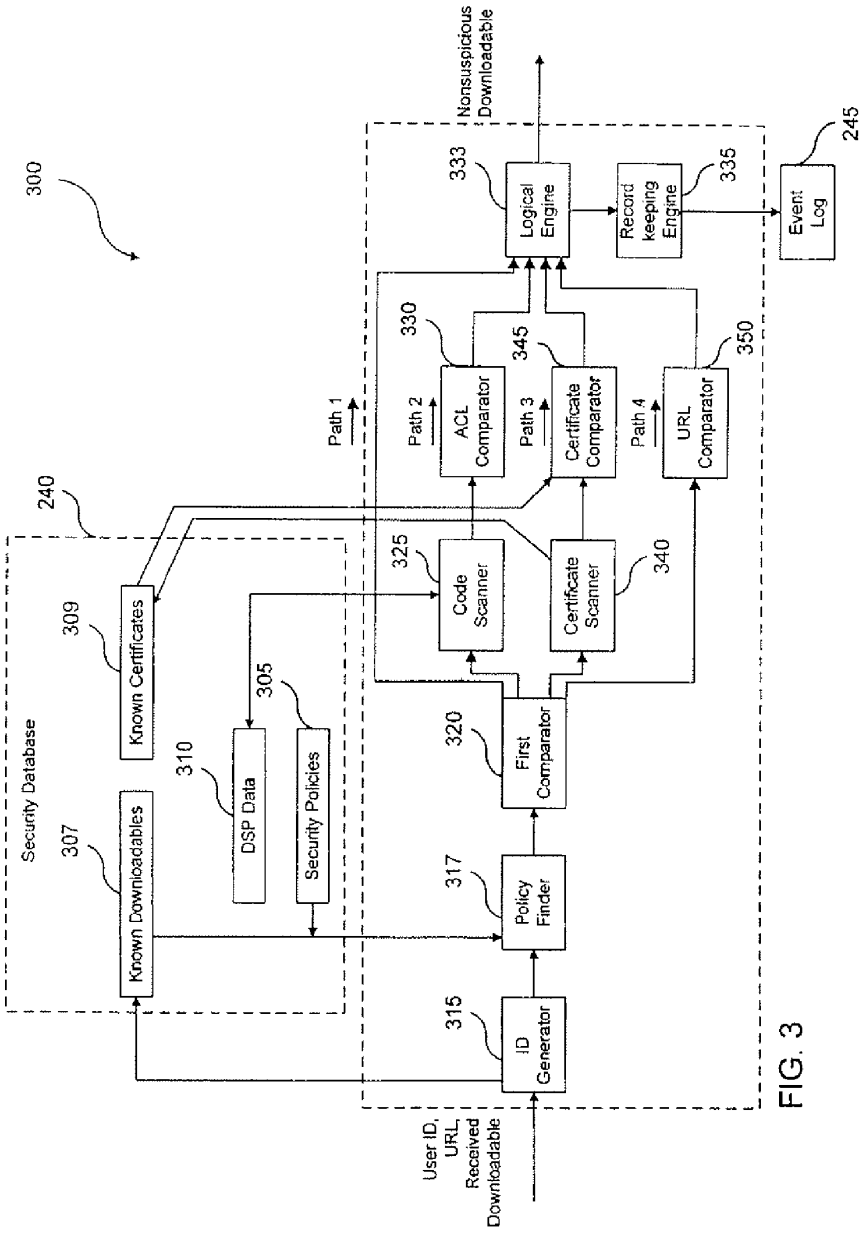

300
240
Security Database
309
Known Certificates
307
Known Downloadables
305
Security Policies
310
DSP Data
Path 1
Path 2
Path 3
Path 4
325
Code Scanner
340
Certificate Scanner
330
ACL Comparator
345
Certificate Comparator
350
URL Comparator
320
First Comparator
317
Policy Finder
315
ID Generator
333
Logical Engine
335
Record keeping Engine
245
Event Log
Nonsuspicious Downloadable
User ID, URL, Received Downloadable

FIG. 3

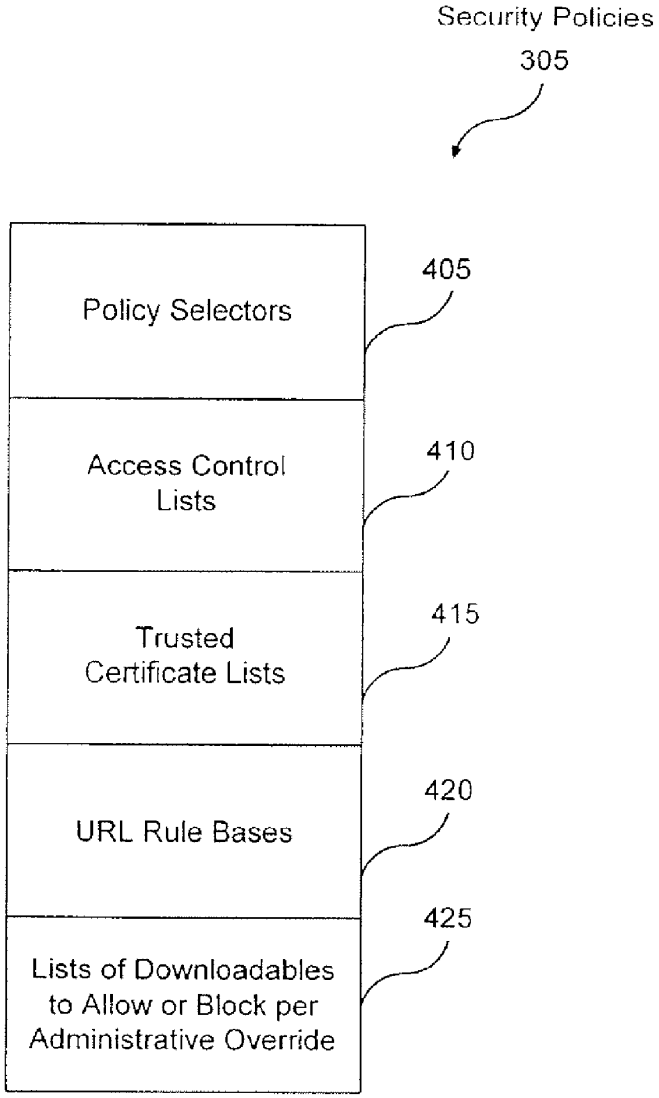

Security Policies
305
Policy Selectors
405
Access Control Lists
410
Trusted Certificate Lists
415
URL Rule Bases
420
Lists of Downloadables to Allow or Block per Administrative Override
425

FIG. 4

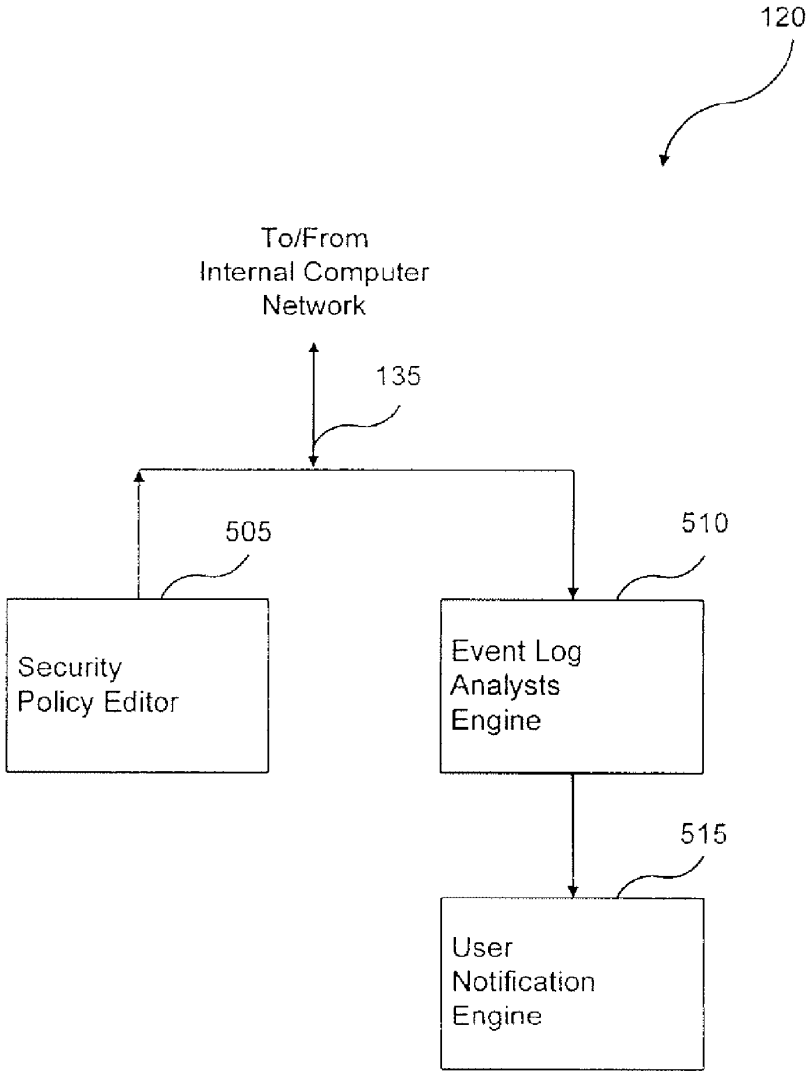

120
To/From
Internal Computer
Network
135
505
510
Security
Policy Editor
Event Log
Analysts
Engine
515
User
Notification
Engine

FIG. 5

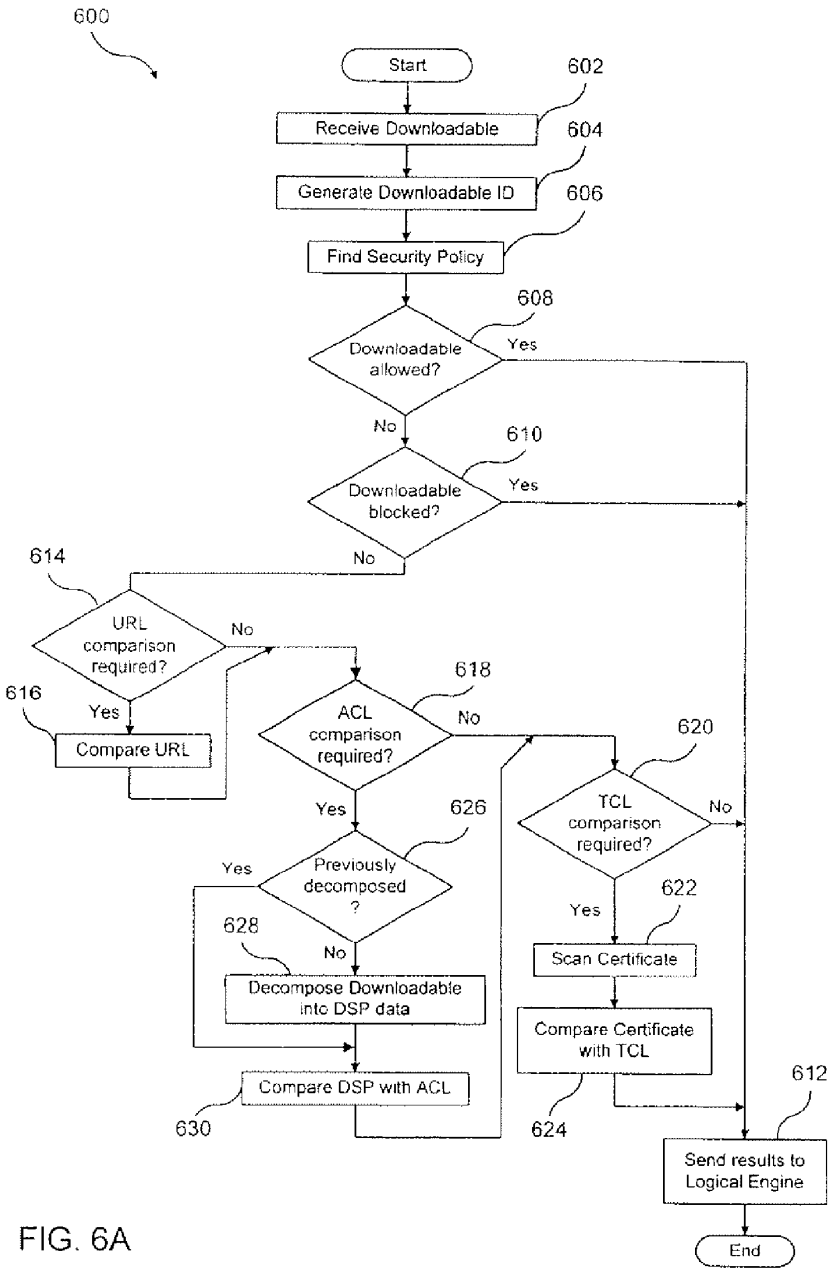

600
Start
602
Receive Downloadable
604
Generate Downloadable ID
606
Find Security Policy
608
Downloadable allowed?
Yes
No
610
Downloadable blocked?
Yes
No
614
URL comparison required?
No
616
Yes
Compare URL
618
ACL comparison required?
No
Yes
626
Previously decomposed ?
Yes
628
No
Decompose Downloadable into DSP data
Compare DSP with ACL
630
620
TCL comparison required?
No
Yes
622
Scan Certificate
Compare Certificate with TCL
624
612
Send results to Logical Engine
End

FIG. 6A

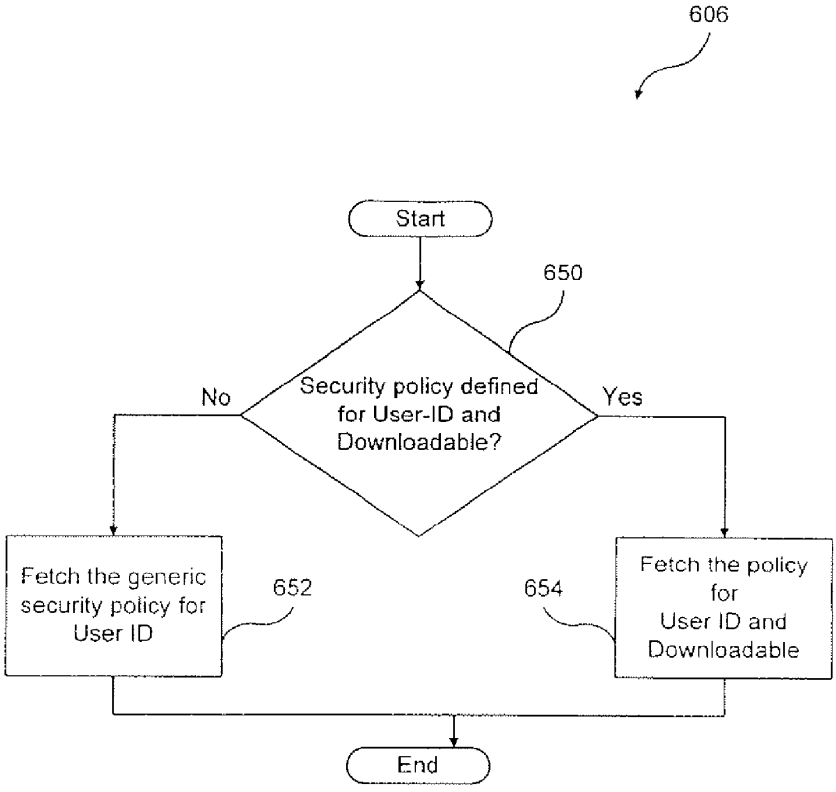

606
Start
650
Security policy defined for User-ID and Downloadable?
No
Yes
Fetch the generic security policy for User ID
652
654
Fetch the policy for User ID and Downloadable
End

FIG. 6B

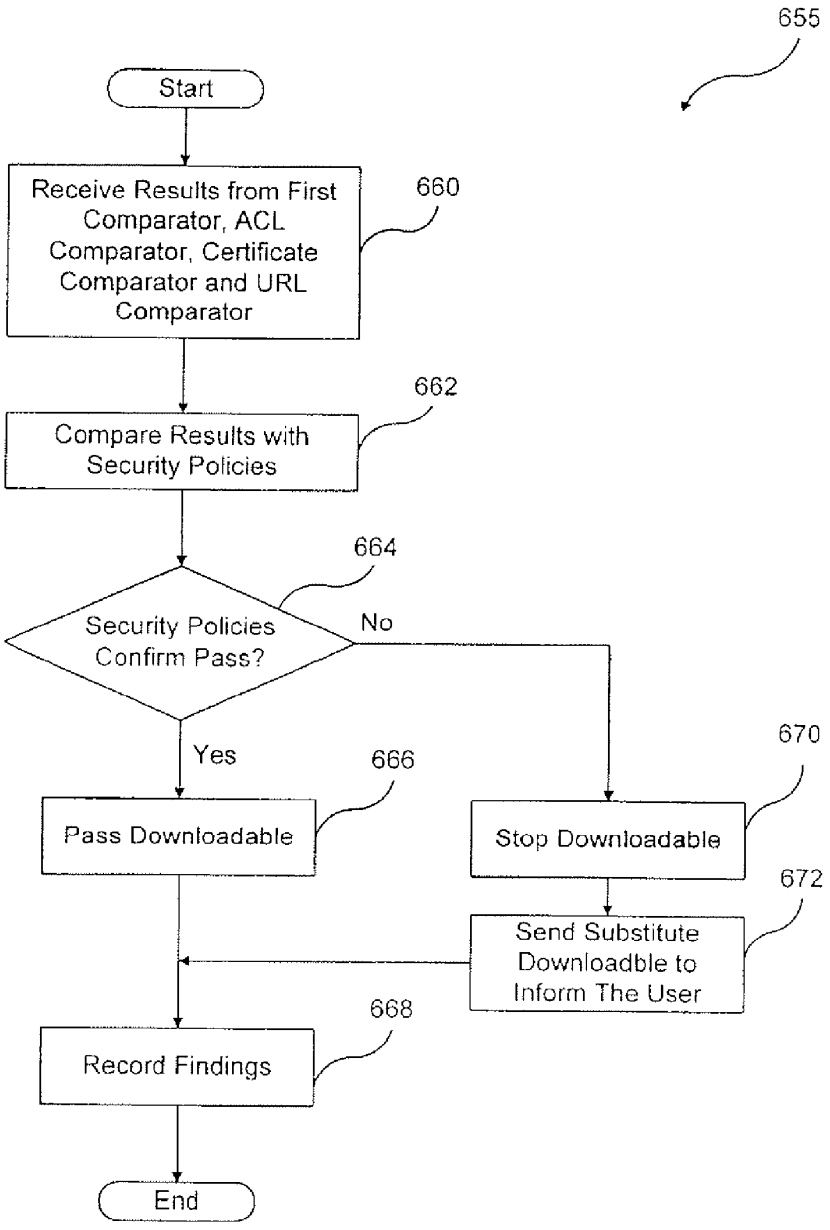

655
Start
Receive Results from First Comparator, ACL Comparator, Certificate Comparator and URL Comparator
660
Compare Results with Security Policies
662
Security Policies Confirm Pass?
664
No
Yes
Pass Downloadable
666
Stop Downloadable
670
Send Substitute Downloadble to Inform The User
672
Record Findings
668
End

FIG. 6C

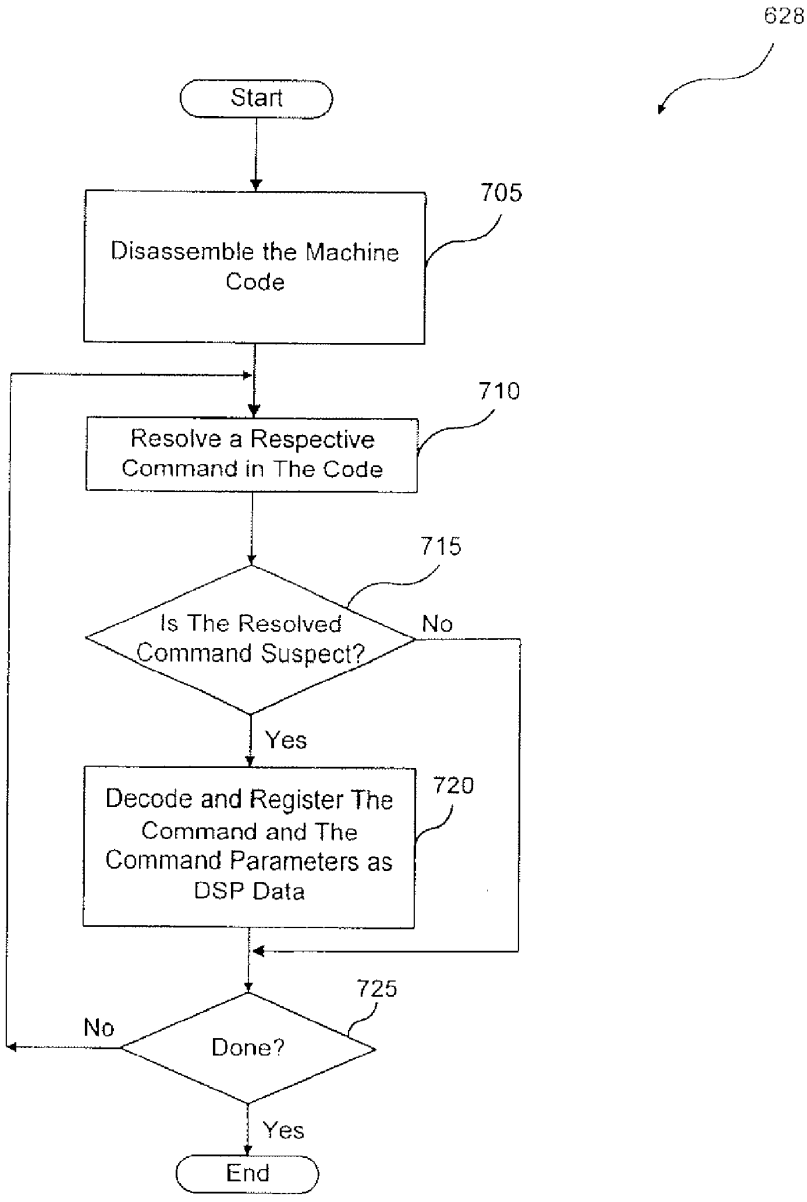

628
Start
705
Disassemble the Machine Code
710
Resolve a Respective Command in The Code
715
Is The Resolved Command Suspect?
No
Yes
720
Decode and Register The Command and The Command Parameters as DSP Data
725
Done?
No
Yes
End

FIG. 7

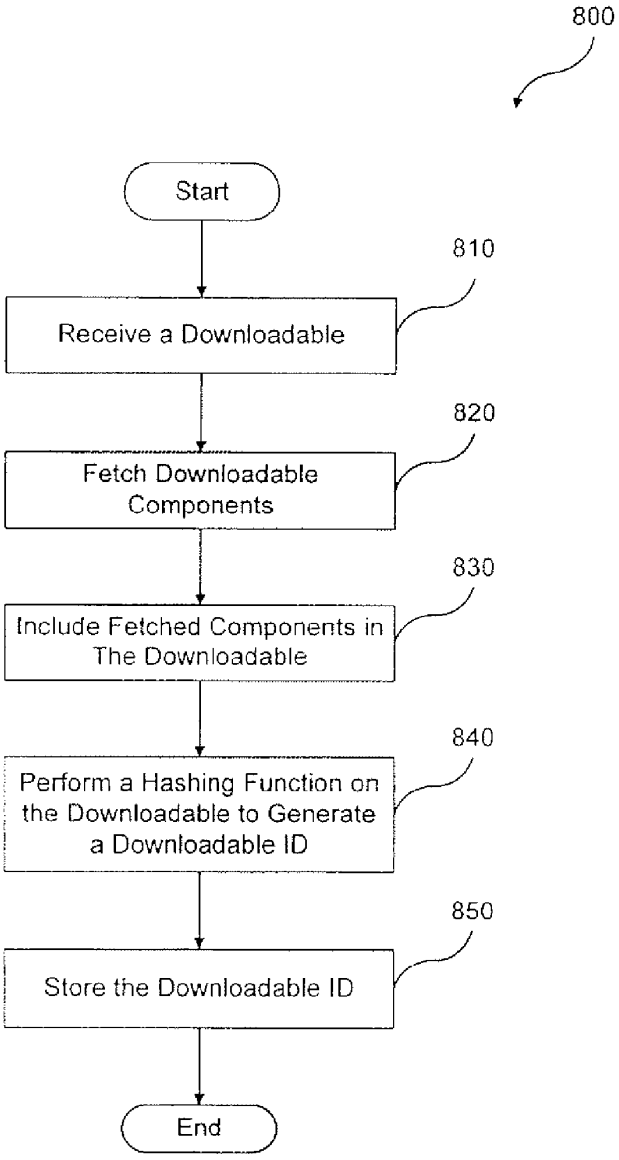

800
Start
810
Receive a Downloadable
820
Fetch Downloadable Components
830
Include Fetched Components in The Downloadable
840
Perform a Hashing Function on the Downloadable to Generate a Downloadable ID
850
Store the Downloadable ID
End

FIG. 8

SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

PRIORITY REFERENCE TO RELATED APPLICATION

This application is a continuation of and hereby incorporates by reference U.S. patent application Ser. No. 08/964,388, entitled "System and Method for Protecting a Computer and a Network from Hostile Downloadables," filed Nov. 6, 1997, which is now U.S. Pat. No. 6,092,194, which claims priority to provisional application Serial No. 60/030,639, entitled "System and Method for Protecting a Computer from Hostile Downloadables," filed on Nov. 8, 1996, by inventor Shlomo Touboul.

INCORPORATION BY REFERENCE TO RELATED APPLICATIONS

This application hereby incorporates by reference related U.S. patent application Ser. No. 08/790,097, entitled "System and Method for Protecting a Client from Hostile Downloadables," filed on Jan. 29, 1997, which is now U.S. Pat. No. 6,167,520, by inventor Shlomo Touboul; and hereby incorporates by reference provisional application Ser. No. 60/030,639, entitled "System and Method for Protecting a Computer from Hostile Downloadables," filed on Nov. 8, 1996, by inventor Shlomo Touboul.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to computer networks, and more particularly provides a system and method for protecting a computer and a network from hostile Downloadables.

2. Description of the Background Art

The Internet is currently a collection of over 100,000 individual computer networks owned by governments, universities, nonprofit groups and companies, and is expanding at an accelerating rate. Because the Internet is public, the Internet has become a major source of many system damaging and system fatal application programs, commonly referred to as "viruses."

Accordingly, programmers continue to design computer and computer network security systems for blocking these viruses from attacking both individual and network computers. On the most part, these security systems have been relatively successful. However, these security systems are not configured to recognize computer viruses which have been attached to or configured as Downloadable application programs, commonly referred to as "Downloadables." A Downloadable is an executable application program, which is downloaded from a source computer and run on the destination computer. Downloadable is typically requested by an ongoing process such as by an Internet browser or web engine. Examples of Downloadables include Java™ applets designed for use in the Java™ distributing environment developed by Sun Microsystems, Inc., JavaScript scripts also developed by Sun Microsystems, Inc., ActiveX™ controls designed for use in the ActiveX™ distributing environment developed by the Microsoft Corporation, and Visual Basic also developed by the Microsoft Corporation. Therefore, a system and method are needed to protect a network from hostile Downloadables.

SUMMARY OF THE INVENTION

The present invention provides a system for protecting a network from suspicious Downloadables. The system comprises a security policy, an interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying the security policy to the Downloadable to determine if the security policy has been violated. The Downloadable may include a Java™ applet, an ActiveX™ control, a JavaScript™ script, or a Visual Basic script. The security policy may include a default security policy to be applied regardless of the client to whom the Downloadable is addressed, a specific security policy to be applied based on the client or the group to which the client belongs, or a specific policy to be applied based on the client/group and on the particular Downloadable received. The system uses an ID generator to compute a Downloadable ID identifying the Downloadable, preferably, by fetching all components of the Downloadable and performing a hashing function on the Downloadable including the fetched components.

Further, the security policy may indicate several tests to perform, including (1) a comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloadables to be blocked or allowed per administrative override; (3) a comparison of the Downloadable security profile data against access control lists; (4) a comparison of a certificate embodied in the Downloadable against trusted certificates; and (5) a comparison of the URL from which the Downloadable originated against trusted and untrusted URLs. Based on these tests, a logical engine can determine whether to allow or block the Downloadable.

The present invention further provides a method for protecting a computer from suspicious Downloadables. The method comprises the steps of receiving a Downloadable, comparing the Downloadable against a security policy to determine if the security policy has been violated, and discarding the Downloadable if the security policy has been violated.

It will be appreciated that the system and method of the present invention may provide computer protection from known hostile Downloadables. The system and method of the present invention may identify Downloadables that perform operations deemed suspicious. The system and method of the present invention may examine the Downloadable code to determine whether the code contains any suspicious operations, and thus may allow or block the Downloadable accordingly.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram illustrating a network system, in accordance with the present invention;

FIG. **2** is a block diagram illustrating details of the internal network security system of FIG. **1**;

FIG. **3** is a block diagram illustrating details of the security program and the security database of FIG. **2**;

FIG. **4** is a block diagram illustrating details of the security policies of FIG. **3**;

FIG. **5** is a block diagram illustrating details of the security management console of FIG. **1**;

FIG. **6A** is a flowchart illustrating a method of examining for suspicious Downloadables, in accordance with the present invention;

FIG. **6B** is a flowchart illustrating details of the step for finding the appropriate security policy of FIG. **6A**;

FIG. **6C** is a flowchart illustrating a method for determining whether an incoming Downloadable is to be deemed suspicious;

FIG. **7** is a flowchart illustrating details of the FIG. **6** step of decomposing a Downloadable; and

FIG. **8** is a flowchart illustrating a method **800** for generating a Downloadable ID for identifying a Downloadable.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. **1** is a block diagram illustrating a network system **100**, in accordance with the present invention. The network system **100** includes an external computer network **105**, such as the Wide Area Network (WAN) commonly referred to as the Internet, coupled via a communications channel **125** to an internal network security system **110**. The network system **100** further includes an internal computer network **115**, such as a corporate Local Area Network (LAN), coupled via a communications channel **130** to the internal network computer system **110** and coupled via a communications channel **135** to a security management console **120**.

The internal network security system **110** examines Downloadables received from external computer network **105**, and prevents Downloadables deemed suspicious from reaching the internal computer network **115**. It will be further appreciated that a Downloadable is deemed suspicious if it performs or may perform any undesirable operation, or if it threatens or may threaten the integrity of an internal computer network **115** component. It is to be understood that the term "suspicious" includes hostile, potentially hostile, undesirable, potentially undesirable, etc. Security management console **120** enables viewing, modification and configuration of the internal network security system **110**.

FIG. **2** is a block diagram illustrating details of the internal network security system **110**, which includes a Central Processing Unit (CPU) **205**, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a signal bus **220**. The internal network security system **110** further includes an external communications interface **210** coupled between the communications channel **125** and the signal bus **220** for receiving Downloadables from external computer network **105**, and an internal communications interface **225** coupled between the signal bus **220** and the communications channel **130** for forwarding Downloadables not deemed suspicious to the internal computer network **115**. The external communications interface **210** and the internal communications interface **225** may be functional components of an integral communications interface (not shown) for both receiving Downloadables from the external computer network **105** and forwarding Downloadables to the internal computer network **115**.

Internal network security system **110** further includes Input/Output (I/O) interfaces **215** (such as a keyboard, mouse and Cathode Ray Tube (CRT) display), a data storage device **230** such as a magnetic disk, and a Random-Access Memory (RAM) **235**, each coupled to the signal bus **220**. The data storage device **230** stores a security database **240**, which includes security information for determining whether a received Downloadable is to be deemed suspicious. The data storage device **230** further stores a users list **260** identifying the users within the internal computer network **115** who may receive Downloadables, and an event log **245** which includes determination results for each Downloadable examined and runtime indications of the internal network security system **110**. An operating system **250** controls processing by CPU **205**, and is typically stored in data storage device **230** and loaded into RAM **235** (as illustrated) for execution. A security program **255** controls examination of incoming Downloadables, and also may be stored in data storage device **230** and loaded into RAM **235** (as illustrated) for execution by CPU **205**.

FIG. **3** is a block diagram illustrating details of the security program **255** and the security database **240**. The security program **255** includes an ID generator **315**, a policy finder **317** coupled to the ID generator **315**, and a first comparator **320** coupled to the policy finder **317**. The first comparator **320** is coupled to a logical engine **333** via four separate paths, namely, via Path **1**, via Path **2**, via Path **3** and via Path **4**. Path **1** includes a direct connection from the first comparator **320** to the logical engine **333**. Path **2** includes a code scanner coupled to the first comparator **320**, and an Access Control List (ACL) comparator **330** coupling the code scanner **325** to the logical engine **333**. Path **3** includes a certificate scanner **340** coupled to the first comparator **320**, and a certificate comparator **345** coupling the certificate scanner **340** to the logical engine **333**. Path **4** includes a Uniform Resource Locator (URL) comparator **350** coupling the first comparator **320** to the logical engine **3330**. A record-keeping engine **335** is coupled between the logical engine **333** and the event log **245**.

The security program **255** operates in conjunction with the security database **240**, which includes security policies **305**, known Downloadables **307**, known Certificates **309** and Downloadable Security Profile (DSP) data **310** corresponding to the known Downloadables **307**. Security policies **305** includes policies specific to particular users **260** and default (or generic) policies for determining whether to allow or block an incoming Downloadable. These security policies **305** may identify specific Downloadables to block, specific Downloadables to allow, or necessary criteria for allowing an unknown Downloadable. Referring to FIG. **4**, security policies **305** include policy selectors **405**, access control lists **410**, trusted certificate lists **415**, URL rule bases **420**, and lists **425** of Downloadables to allow or to block per administrative override.

Known Downloadables **307** include lists of Downloadables which Original Equipment Manufacturers (OEMs) know to be hostile, of Downloadables which OEMs know to be non-hostile, and of Downloadables previously received by this security program **255**. DSP data **310** includes the list of all potentially hostile or suspicious computer operations that may be attempted by each known Downloadable **307**, and may also include the respective arguments of these operations. An identified argument of an operation is referred to as "resolved." An unidentified argument is referred to as "unresolved." DSP data **310** is described below with reference to the code scanner **325**.

The ID generator **315** receives a Downloadable (including the URL from which it came and the userID of the intended recipient) from the external computer network **105** via the external communications interface **210**, and generates a Downloadable ID for identifying each Downloadable. The Downloadable ID preferably includes a digital hash of the complete Downloadable code. The ID generator **315** preferably prefetches all components embodied in or identified by the code for Downloadable ID generation. For example, the ID generator **315** may prefetch all classes embodied in or identified by the Java™ applet bytecode to generate the Downloadable ID. Similarly, the ID generator **315** may retrieve all components listed in the INF file for an ActiveX™ control to compute a Downloadable ID. Accordingly, the Downloadable ID for the Downloadable will be the same each time the ID generator **315** receives the same Downloadable. The ID generator **315** adds the generated Downloadable ID to the list of known Downloadables

307 (if it is not already listed). The ID generator 315 then forwards the Downloadable and Downloadable ID to the policy finder 317.

The policy finder 317 uses the userID of the intended user and the Downloadable ID to select the specific security policy 305 that shall be applied on the received Downloadable. If there is a specific policy 305 that was defined for the user (or for one of its super groups) and the Downloadable, then the policy is selected. Otherwise the generic policy 305 that was defined for the user (or for one of its super groups) is selected. The policy finder 317 then sends the policy to the first comparator 320.

The first comparator 320 receives the Downloadable, the Downloadable ID and the security policy 305 from the policy finder 317. The first comparator 320 examines the security policy 305 to determine which steps are needed for allowing the Downloadable. For example, the security policy 305 may indicate that, in order to allow this Downloadable, it must pass all four paths, Path 1, Path 2, Path 3 and Path 4. Alternatively, the security policy 305 may indicate that to allow the Downloadable, the it must pass only one of the paths. The first comparator 320 responds by forwarding the proper information to the paths identified by the security policy 305.

Path 1

In path 1, the first comparator 320 checks the policy selector 405 of the security policy 305 that was received from the policy finder 317. If the policy selector 405 is either "Allowed" or "Blocked," then the first comparator 320 forwards this result directly to the logical engine 333. Otherwise, the first comparator 320 invokes the comparisons in path2 and/or path 3 and/or path 4 based on the contents of policy selector 405. It will be appreciated that the first comparator 320 itself compares the Downloadable ID against the lists of Downloadables to allow or block per administrative override 425. That is, the system security administrator can define specific Downloadables as "Allowed" or "Blocked."

Alternatively, the logical engine 333 may receive the results of each of the paths and based on the policy selector 405 may institute the final determination whether to allow or block the Downloadable. The first comparator 320 informs the logical engine 333 of the results of its comparison.

Path 2

In path 2, the first comparator 320 delivers the Downloadable, the Downloadable ID and the security policy 305 to the code scanner 325. If the DSP data 310 of the received Downloadable is known, the code scanner 325 retrieves and forwards the information to the ACL comparator 330. Otherwise, the code scanner 325 resolves the DSP data 310. That is, the code scanner 325 uses conventional parsing techniques to decompose the code (including all prefetched components) of the Downloadable into the DSP data 310. DSP data 310 includes the list of all potentially hostile or suspicious computer operations that may be attempted by a specific Downloadable 307, and may also include the respective arguments of these operations. For example, DSP data 310 may include a READ from a specific file, a SEND to an unresolved host, etc. The code scanner 325 may generate the DSP data 310 as a list of all operations in the Downloadable code which could ever be deemed potentially hostile and a list of all files to be accessed by the Downloadable code. It will be appreciated that the code scanner 325 may search the code for any pattern, which is undesirable or suggests that the code was written by a hacker.

An Example List of Operations Deemed Potentially Hostile

File operations: READ a file, WRITE a file;

Network operations: LISTEN on a socket, CONNECT to a socket, SEND data, RECEIVE data, VIEW INTRANET;

Registry operations: READ a registry item, WRITE a registry item;

Operating system operations: EXIT WINDOWS, EXIT BROWSER, START PROCESS/THREAD, KILL PROCESS/THREAD, CHANGE PROCESS/THREAD PRIORITY, DYNAMICALLY LOAD A CLASS/LIBRARY, etc.; and

Resource usage thresholds: memory, CPU, graphics, etc.

In the preferred embodiment, the code scanner 325 performs a full-content inspection. However, for improved speed but reduced security, the code scanner 325 may examine only a portion of the Downloadable such as the Downloadable header. The code scanner 325 then stores the DSP data into DSP data 310 (corresponding to its Downloadable ID), and sends the Downloadable, the DSP data to the ACL comparator 330 for comparison with the security policy 305.

The ACL comparator 330 receives the Downloadable, the corresponding DSP data and the security policy 305 from the code scanner 325, and compares the DSP data against the security policy 305. That is, the ACL comparator 330 compares the DSP data of the received Downloadable against the access control lists 410 in the received security policy 305. The access control list 410 contains criteria indicating whether to pass or fail the Downloadable. For example, an access control list may indicate that the Downloadable fails if the DSP data includes a WRITE command to a system file. The ACL comparator 330 sends its results to the logical engine 333.

Path 3

In path 3, the certificate scanner 340 determines whether the received Downloadable was signed by a certificate authority, such as VeriSign, Inc., and scans for a certificate embodied in the Downloadable. The certificate scanner 340 forwards the found certificate to the certificate comparator 345. The certificate comparator 345 retrieves known certificates 309 that were deemed trustworthy by the security administrator and compares the found certificate with the known certificates 309 to determine whether the Downloadable was signed by a trusted certificate. The certificate comparator 345 sends the results to the logical engine 333.

Path 4

In path 4, the URL comparator 350 examines the URL identifying the source of the Downloadable against URLs stored in the URL rule base 420 to determine whether the Downloadable comes from a trusted source. Based on the security policy 305, the URL comparator 350 may deem the Downloadable suspicious if the Downloadable comes from an untrustworthy source or if the Downloadable did not come from a trusted source. For example, if the Downloadable comes from a known hacker, then the Downloadable may be deemed suspicious and presumed hostile. The URL comparator 350 sends its results to the logical engine 333.

The logical engine 333 examines the results of each of the paths and the policy selector 405 in the security policy 305 to determine whether to allow or block the Downloadable. The policy selector 405 includes a logical expression of the results received from each of the paths. For example, the

logical engine **333** may block a Downloadable if it fails any one of the paths, i.e., if the Downloadable is known hostile (Path **1**), if the Downloadable may request suspicious operations (Path **2**), if the Downloadable was not signed by a trusted certificate authority (Path **3**), or if the Downloadable did came from an untrustworthy source (Path **4**). The logical engine **333** may apply other logical expressions according to the policy selector **405** embodied in the security policy **305**. If the policy selector **405** indicates that the Downloadable may pass, then the logical engine **333** passes the Downloadable to its intended recipient. Otherwise, if the policy selector **405** indicates that the Downloadable should be blocked, then the logical engine **333** forwards a non-hostile Downloadable to the intended recipient to inform the user that internal network security system **110** discarded the original Downloadable. Further, the logical engine **333** forwards a status report to the record-keeping engine **335**, which stores the reports in event log **245** in the data storage device **230** for subsequent review, for example, by the MIS director.

FIG. **5** is a block diagram illustrating details of the security management console **120**, which includes a security policy editor **505** coupled to the communications channel **135**, an event log analysis engine **510** coupled between communications channel **135** and a user notification engine **515**, and a Downloadable database review engine **520** coupled to the communications channel **135**. The security management console **120** further includes computer components similar to the computer components illustrated in FIG. **2**.

The security policy editor **505** uses an I/O interface similar to I/O interface **215** for enabling authorized user modification of the security policies **305**. That is, the security policy editor **505** enables the authorized user to modify specific security policies **305** corresponding to the users **260**, the default or generic security policy **305**, the Downloadables to block per administrative override, the Downloadables to allow per administrative override, the trusted certificate lists **415**, the policy selectors **405**, the access control lists **410**, the URLs in the URL rule bases **420**, etc. For example, if the authorized user learns of a new hostile Downloadable, then the user can add the Downloadable to the Downloadables to block per system override.

The event log analysis engine **510** examines the status reports contained in the event log **245** stored in the data storage device **230**. The event log analysis engine **510** determines whether notification of the user (e.g., the security system manager or MIS director) is warranted. For example, the event log analysis engine **510** may warrant user notification whenever ten (10) suspicious Downloadables have been discarded by internal network security system **110** within a thirty (30) minute period, thereby flagging a potential imminent security threat. Accordingly, the event log analysis engine **510** instructs the user notification engine **515** to inform the user. The user notification engine **515** may send an e-mail via internal communications interface **220** or via external communications interface **210** to the user, or may display a message on the user's display device (not shown).

FIG. **6A** is a flowchart illustrating a method **600** for protecting an internal computer network **115** from suspicious Downloadables. Method **600** begins with the ID generator **315** in step **602** receiving a Downloadable. The ID generator **315** in step **604** generates a Downloadable ID identifying the received Downloadable, preferably, by generating a digital hash of the Downloadable code (including prefetched components). The policy finder **317** in step **606** finds the appropriate security policy **305** corresponding to the userID specifying intended recipient (or the group to which the intended recipient belongs) and the Downloadable. The selected security policy **305** may be the default security policy **305**. Step **606** is described in greater detail below with reference to FIG. **6B**.

The first comparator **320** in step **608** examines the lists of Downloadables to allow or to block per administrative override **425** against the Downloadable ID of the incoming Downloadable to determine whether to allow the Downloadable automatically. If so, then in step **612** the first comparator **320** sends the results to the logical engine **333**. If not, then the method **600** proceeds to step **610**. In step **610**, the first comparator **620** examines the lists of Downloadables to block per administrative override **425** against the Downloadable ID of the incoming Downloadable for determining whether to block the Downloadable automatically. If so, then the first comparator **420** in step **612** sends the results to the logical engine **333**. Otherwise, method **600** proceeds to step **614**.

In step **614**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path **4**. If not, then method **600** jumps to step **618**. If so, then the URL comparator **350** in step **616** compares the URL embodied in the incoming Downloadable against the URLs of the URL rules bases **420**, and then method **600** proceeds to step **618**.

In step **618**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path **2**. If not, then method **600** jumps to step **620**. Otherwise, the code scanner **235** in step **626** examines the DSP data **310** based on the Downloadable ID of the incoming Downloadable to determine whether the Downloadable has been previously decomposed. If so, then method **600** jumps to step **630**. Otherwise, the code scanner **325** in step **628** decomposes the Downloadable into DSP data. Downloadable decomposition is described in greater detail with reference to FIG. **7**. In step **630**, the ACL comparator **330** compares the DSP data of the incoming Downloadable against the access control lists **410** (which include the criteria necessary for the Downloadable to fail or pass the test).

In step **620**, the first comparator **320** determines whether the security policy **305** indicates that the Downloadable should be tested according to Path **3**. If not, then method **600** returns to step **612** to send the results of each of the test performed to the logical engine **333**. Otherwise, the certificate scanner **622** in step **622** scans the Downloadable for an embodied certificate. The certificate comparator **345** in step **624** retrieves trusted certificates from the trusted certificate lists (TCL) **415** and compares the embodied certificate with the trusted certificates to determine whether the Downloadable has been signed by a trusted source. Method **600** then proceeds to step **612** by the certificate scanner **345** sending the results of each of the paths taken to the logical engine **333**. The operations of the logical engine **333** are described in greater detail below with reference to FIG. **6C**. Method **600** then ends.

One skilled in the art will recognize that the tests may be performed in a different order, and that each of the tests need not be performed. Further, one skilled in the art will recognize that, although path **1** is described in FIG. **6A** as an automatic allowance or blocking, the results of Path **1** may be another predicate to be applied by the logical engine **333**. Further, although the tests are shown serially in FIG. **6A**, the tests may be performed in parallel as illustrated in FIG. **3**.

FIG. 6B is a flowchart illustrating details of step **606** of FIG. 6A (referred to herein as method **606**). Method **606** begins with the policy finder **317** in step **650** determining whether security policies **305** include a specific security policy corresponding to the userID and the Downloadable. If so, then the policy finder **317** in step **654** fetches the corresponding specific policy **305**. If not, then the policy finder **317** in step **652** fetches the default or generic security policy **305** corresponding to the userID. Method **606** then ends.

FIG. 6C is a flowchart illustrating details of a method **655** for determining whether to allow or to block the incoming Downloadable. Method **655** begins with the logical engine **333** in step **660** receiving the results from the first comparator **320**, from the ACL comparator **330**, from the certificate comparator **345** and from the URL comparator **350**. The logical engine **333** in step **662** compares the results with the policy selector **405** embodied in the security policy **305**, and in step **664** determines whether the policy selector **405** confirms the pass. For example, the policy selector **405** may indicate that the logical engine **333** pass the Downloadable if it passes one of the tests of Path **1**, Path **2**, Path **3** and Path **4**. If the policy selector **405** indicates that the Downloadable should pass, then the logical engine **333** in step **666** passes the Downloadable to the intended recipient. In step **668**, the logical engine **333** sends the results to the record-keeping engine **335**, which in turn stores the results in the event log **245** for future review. Method **655** then ends. Otherwise, if the policy selector **405** in step **664** indicates that the Downloadable should not pass, then the logical engine **333** in step **670** stops the Downloadable and in step **672** sends a non-hostile substitute Downloadable to inform the user that the incoming Downloadable has been blocked. Method **655** then jumps to step **668**.

FIG. 7 is a flowchart illustrating details of step **628** of FIG. 6A (referred to herein as method **628**) for decomposing a Downloadable into DSP data **310**. Method **628** begins in step **705** with the code scanner **325** disassembling the machine code of the Downloadable. The code scanner **325** in step **710** resolves a respective command in the machine code, and in step **715** determines whether the resolved command is suspicious (e.g., whether the command is one of the operations identified in the list described above with reference to FIG. **3**). If not, then the code scanner **325** in step **725** determines whether it has completed decomposition of the Downloadable, i.e., whether all operations in the Downloadable code have been resolved. If so, then method **628** ends. Otherwise, method **628** returns to step **710**.

Otherwise, if the code scanner **325** in step **71** determines that the resolved command is suspect, then the code scanner **325** in step **720** decodes and registers the suspicious command and its command parameters as DSP data **310**. The code scanner **325** in step **720** registers the commands and command parameters into a format based on command class (e.g., file operations, network operations, registry operations, operating system operations, resource usage thresholds). Method **628** then jumps to step **725**.

FIG. **8** is a flowchart illustrating a method **800** for generating a Downloadable ID for identifying a Downloadable. Method **800** begins with the ID generator **315** in step **810** receiving a Downloadable from the external computer network **105**. The ID generator **315** in step **820** may fetch some or all components referenced in the Downloadable code, and in step **830** includes the fetched components in the Downloadable code. The ID generator **315** in step **840** performs a hashing function on at least a portion of the Downloadable code to generate a Downloadable ID. The ID generator **315** in step **850** stores the generated Downloadable ID in the security database **240** as a reference to the DSP data **310**. Accordingly, the Downloadable ID will be the same for the identical Downloadable each time it is encountered.

The foregoing description of the preferred embodiments of the invention is by way of example only, and other variations of the above-described embodiments and methods are provided by the present invention. For example, although the invention has been described in a system for protecting an internal computer network, the invention can be embodied in a system for protecting an individual computer. Components of this invention may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. The embodiments described herein have been presented for purposes of illustration and are not intended to be exhaustive or limiting. Many variations and modifications are possible in light of the foregoing teaching. The system is limited only by the following claims.

What is claimed is:

1. A computer-based method for generating a Downloadable ID to identify a Downloadable, comprising:

obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;

fetching at least one software component identified by the one or more references; and

performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

2. The method of claim **1**, wherein the Downloadable includes an applet.

3. The method of claim **1**, wherein the Downloadable includes an active software control.

4. The method of claim **1**, wherein the Downloadable includes a plugin.

5. The method of claim **1**, wherein the Downloadable includes HTML code.

6. The method of claim **1**, wherein the Downloadable includes an application program.

7. The method of claim **1**, wherein said fetching includes fetching a first software component referenced by the Downloadable.

8. The method of claim **1**, wherein said fetching includes fetching all software components referenced by the Downloadable.

9. A system for generating a Downloadable ID to identify a Downloadable, comprising:

a communications engine for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable; and

an ID generator coupled to the communications engine that fetches at least one software component identified by the one or more references, and for performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

10. The system of claim **9**, wherein the Downloadable includes an applet.

11. The system of claim **9**, wherein the Downloadable includes an active software control.

12. The system of claim **9**, wherein the Downloadable includes a plugin.

13. The system of claim **9**, wherein the Downloadable includes HTML code.

14. The system of claim 9, wherein the Downloadable includes an application program.

15. The system of claim 9, wherein the ID generator fetches a first software component referenced by the Downloadable.

16. The method of claim 9, wherein the ID generator fetches all software components referenced by the Downloadable.

17. A system for generating a Downloadable ID to identify a Downloadable, comprising:

means for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;

means for fetching at least one software component identified by the one or more references; and

means for performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

18. A computer-readable storage medium storing program code for causing a computer to perform the steps of:

obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;

fetching at least one software component identified by the one or more references; and

performing a hashing function on the Downloadable and the fetched software components to generate a Downloadable ID.

* * * * *

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
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.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	3

Patent Number Issued Date	6,804,780 October 12, 2004
Application Number Filing Date	09/539,667 October 12, 2004
First Named Inventor	Shlomo TOUBOUL
Art Unit	2131
Examiner Name	C. REVAK
Attorney Docket Number	43426.00011

ENCLOSURES ***(check all that apply)***

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) ____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☒ Change of Correspondence Address [Total 1 page]
- ☒ Other Enclosure(s) *(please identify below)*:

Return postcard

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to **Deposit Account Number 05-0150**.

I have enclosed a duplicate copy of this sheet. [Total 2 pages]

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm	Squire, Sanders & Dempsey L.L.P. 600 Hansen Way Palo Alto, CA 94304-1043		
Signature			
Printed Name	Marc A. Sockol		
Date	April 14, 2005	Reg. No.	40,823

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Signature	Cathi L.G. Thoorsell		
Typed or printed name	Cathi L.G. Thoorsell	Date	April 14, 2005

This collection of information is required by 37 CFR 1.5. 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 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.

PaloAlto/82599.1

COPY

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
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.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	3

Patent Number Issued Date	6,804,780 October 12, 2004
Application Number Filing Date	09/539,667 October 12, 2004
First Named Inventor	Shlomo TOUBOUL
Art Unit	2131
Examiner Name	C. REVAK
Attorney Docket Number	43426.00011

ENCLOSURES ***(check all that apply)***

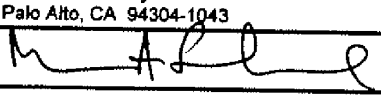
- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) ____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☒ Change of Correspondence Address [Total 1 page]
- ☒ Other Enclosure(s) *(please identify below)*:

Return postcard

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to **Deposit Account Number 05-0150**.

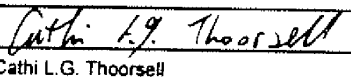
I have enclosed a duplicate copy of this sheet. [Total 2 pages]

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm	Squire, Sanders & Dempsey L.L.P. 600 Hansen Way Palo Alto, CA 94304-1043		
Signature			
Printed Name	Marc A. Sockol		
Date	April 14, 2005	Reg. No.	40,823

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Signature			
Typed or printed name	Cathi L.G. Thoorsell	Date	April 14, 2005

This collection of information is required by 37 CFR 1.5. 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 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.

PaloAlto/82599.1

PTO/SB/123 (09-04)
Approved for use through 11/30/2005. OMB 0651-0035
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
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.

CHANGE OF CORRESPONDENCE ADDRESS
Patent

Address to:

Mail Stop Post Issue
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Patent Number	6,804,780
Issue Date	October 12, 2004
Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo TOUBOUL
Attorney Docket Number	43426.00011

Please change the Correspondence Address for the above-identified patent to:

☐ The address associated with Customer Number ____

OR

☒ **Firm *or* Individual Name**	EITAN LAW GROUP		
Address	7 SHENKAR ST. POB 2081		
City	HERZLIA	**State**	**ZIP** 46120
Country	ISRAEL		
Telephone	972-9-972-6000	**Fax**	972-9-972-6001

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124)

This form will not affect any "fee address" provided for the above-identified patent. To change a "fee address" use the "Fee Address Indication Form" (PTO/SB/47).

I am the :

☐ Patentee.

☐ Assignee of record of the entire interest. See 37 CFR 3.71.
Certificate under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

☒ Attorney or agent of record. Registration Number 40,823

Signature	Marc A. Sockol		
Typed or Printed Name	M A Sockol		
Date	April 14, 2005	Telephone	650-856-6500

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 one form is submitted.

This collection of information is required by 37 CFR 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.**

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

PaloAlto/82599.1

U.S DEPARTMENT OF COMMERCE
PATENT/TRADEMARK OFFICE
WASHINGTON, D.C. 20231

Squire, Sanders & Dempsey L.L.P.
600 Hansen Way
Palo Alto, CA 94304-1043

Date Mailed: April 14, 2005		By: MAS/ct	PTO DATE STAMP:	
Application No.:	09/539,667	Filed:	March 30, 2000	Docket No.: 43426.00011
Patent No.:	6,804,780	Issued:	October 12, 2004	
Applicant:	Shlomo TOUBOUL			

Title: SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

The following has been received in the U.S. Patent Office on the date stamped hereon:

- ☐ Patent Application ___ Pages ___ Claims
- ☐ Drawings Informal ___ Sheets
- ☐ General Authorization / Request to Petition for Extensions of Time
- ☐ Oath/Declaration
- ☐ Assignment & Recordation Cover Sheet
- ☐ Verified Statement Claiming Small Entity Status
- ☐ Continued Prosecution Application (§1.53(d)
- ☐ Provisional Application _____ Pages
- ☐ Design Application ___ Pages ___ Drawings
- ☐ Power of Attorney
- ☒ Certificate(s) of First Class Mailing
- ☐ Response/Amendment
- ☐ Petition for Extension of Time
- ☒ Transmittal Form w/ duplication [Total 2 pages]
- ☒ Change of Correspondence [Total 1 page]
- ☐ Fee Transmittal (in duplicate)
- ☐ Issue Fee Transmittal with PTO-85b
- ☐ Copy of PTO-1533, Notice to File Missing Parts
- ☐ Info. Disclosure Statement & PTO-1449/Refs ___
- ☒ This postcard

PaloAlto/82599.1

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.
09/539,667	10/12/2004	6804780	40492.00011	8436

30256 7590 09/23/2004

SQUIRE, SANDERS & DEMPSEY L.L.P
600 HANSEN WAY
PALO ALTO, CA 94304-1043

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Extension under 35 U.S.C. 154 (b)
(application filed after June 7, 1995 but prior to May 29, 2000)

The Patent Term Extension is 0 day(s). Any patent to issue from the above-identified application will include an indication of the 0 day extension on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Extension is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (703) 305-1383. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (703) 305-8283.

APPLICANT(s) (up to 18 names are included below, see PAIR WEB site http://pair.uspto.gov for additional applicants):

Shlomo Touboul, Kefar-haim, ISRAEL;

DATE ENTERED: _____
No Action

CALENDARED
BY: MO
ATTORNEY
SQUIRE SANDERS & DEMPSEY

IR103 (Rev. 11/03)

Date Mailed: August 31, 2004 | By: MAS/emj | PTO DATE STAMP:

Application No.: 09/539,667 | Docket No.: 43426.00011

Applicant: Shlomo Touboul

Title: SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

The following has been received in the U.S. Patent Office on the date stamped hereon:

- ☐ Patent Application __ Pages __ Claims
- ☐ Drawings Informal ____ Sheets
- ☐ General Authorization / Request to Petition for Extensions of Time
- ☐ Oath/Declaration
- ☐ Assignment & Recordation Cover Sheet
- ☐ Verified Statement Claiming Small Entity Status
- ☐ Continued Prosecution Application (§1.53(d)
- ☐ Provisional Application _____ Pages
- ☐ Design Application __ Pages __ Drawings
- ☐ Status Letter
- ☐ Check No. for $
- ☐ Power of Attorney
- ☒ Certificate(s) of First Class Mailing
- ☐ Response/Amendment
- ☐ Petition for Extension of Time
- ☒ Transmittal Form
- ☐ Notice of Appeal
- ☐ Fee Transmittal (in duplicate)
- ☒ Issue Fee Transmittal with PTO-85b (in duplicate)
- ☐ Copy of PTO-1533, Notice to File Missing Parts
- ☐ Info. Disclosure Statement & PTO-1449/Refs ___
- ☐ Request to Correct Filing Receipt
- ☐ Check No. for $
- ☒ Other: Authorization to Charge Deposit Account No. 05-0150 ($1,330 Issue Fee)

U.S DEPARTMENT OF COMMERCE
PATENT/TRADEMARK OFFICE
WASHINGTON, D.C. 20231

Squire, Sanders & Dempsey L.L.P.
600 Hansen Way, Suite 100
Palo Alto, CA 94304-1043

PTO/SB/21 (04-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
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.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Art Unit	2131
Examiner Name	Christopher A. Revak
Total Number of Pages in This Submission: 3	Attorney Docket Number: 43426.00011

ENCLOSURES ***(check all that apply)***

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Formal Drawings
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☒ PTOL-85 Issue Fee Transmittal (in duplicate)
- ☒ Authorization to Charge Deposit Account No. 05-0150 $240 Issue Fee
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance Communication to Technology Center (TC)
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☒ Return Postcard
- ☐ Other Enclosure(s) *(please identify below).*

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Marc A. Sockol, Reg. No. 40,823 Squire, Sanders & Dempsey, L.L.P. 600 Hansen Way Palo Alto, CA 94304-1043
Signature	
Date	August 31, 2004

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Eileen M. Janikowski		
Signature		Date	August 31, 2004

This collection of information is required by 37 CFR 1.5. 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 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.

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 (703) 746-4000

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 4 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: Legibly mark-up with any corrections or use Block 1)

30256 7590 06/04/2004

SQUIRE, SANDERS & DEMPSEY L.L.P
600 HANSEN WAY
PALO ALTO, CA 94304-1043

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.

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, on the date indicated below.

Eileen M. Janikowski	(Depositor's name)
Eileen Janikowski	(Signature)
August 31, 2004	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/539,667	03/30/2000	Shlomo Touboul	~~40492.00011~~ 43426.00011	8436

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	~~YES~~ NO	$665 1330	$0	$665 1330	09/07/2004

EXAMINER	ART UNIT	CLASS-SUBCLASS
REVAK, CHRISTOPHER A	2131	713-181000

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.

1 Squire, Sanders & Dempsey, L.L.P.
2
3

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. Inclusion of assignee data is only appropriate when an assignment has been previously submitted to the USPTO or is being submitted under separate cover. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: FINJAN SOFTWARE, LTD.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): NETANYA, ISRAEL

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 enclosed:

☒ Issue Fee

☐ Publication Fee

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s):

☐ A check in the amount of the fee(s) is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Director is hereby authorized by charge the required fee(s), or credit any overpayment, to Deposit Account Number 05-0150 (enclose an extra copy of this form).

Director for Patents is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above.

(Authorized Signature) _____ (Date) August 25, 2004
Marc A. Sockol, Reg. No. 40,823

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.

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, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, 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.

TRANSMIT THIS FORM WITH FEE(S)

COPY

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 (703) 746-4000

COPY

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 4 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: Legibly mark-up with any corrections or use Block 1)

30256 7590 06/04/2004

SQUIRE, SANDERS & DEMPSEY L.L.P
600 HANSEN WAY
PALO ALTO, CA 94304-1043

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.

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, on the date indicated below.

Eileen M. Janikowski	(Depositor's name)
Eileen Janikowski	(Signature)
August 31, 2004	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/539,667	03/30/2000	Shlomo Touboul	~~40492.00011~~ 43426.00011	8436

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	~~YES~~ NO	~~$665~~ 1330	$0	~~$665~~ 1330	09/07/2004

EXAMINER	ART UNIT	CLASS-SUBCLASS
REVAK, CHRISTOPHER A	2131	713-181000

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.

1 Squire, Sanders & Dempsey, L.L.P.
2
3

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. Inclusion of assignee data is only appropriate when an assignment has been previously submitted to the USPTO or is being submitted under separate cover. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: FINJAN SOFTWARE, LTD.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): NETANYA, ISRAEL

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 enclosed:

☒ Issue Fee

☐ Publication Fee

☐ Advance Order - # of Copies _____

4b. Payment of Fee(s):

☐ A check in the amount of the fee(s) is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Director is hereby authorized by charge the required fee(s), or credit any overpayment, to Deposit Account Number 05-0150 (enclose an extra copy of this form).

Director for Patents is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above.

(Authorized Signature) _____ (Date) August 25, 2004

Marc A. Sockol, Reg. No. 40,823

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.

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, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, 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.

TRANSMIT THIS FORM WITH FEE(S)

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

Issue Fee Due: 9/7/04

30256 7590 06/04/2004

SQUIRE, SANDERS & DEMPSEY L.L.P
600 HANSEN WAY
PALO ALTO, CA 94304-1043

JUN 0 7 2004

CALENDARED
BY cdy
ATTORNEY
SQUIRE, SANDERS & DEMPSEY

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 06/04/2004

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/539,667	03/30/2000	Shlomo Touboul	~~40492~~.00011 9326	8436

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	~~YES~~ NO	~~$665~~ 1335	$0	~~$665~~ 1335	09/07/2004

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 REFLECTS A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE APPLIED IN THIS APPLICATION. THE PTOL-85B (OR AN EQUIVALENT) MUST BE RETURNED WITHIN THIS PERIOD EVEN IF NO FEE IS DUE OR THE APPLICATION WILL BE REGARDED AS ABANDONED.

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 is changed, pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above and notify the United States Patent and Trademark Office of the change in status, 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 the box below and enclose the PUBLICATION FEE and 1/2 the ISSUE FEE shown above.

☐ Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

II. PART B - FEE(S) TRANSMITTAL should be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). Even if the fee(s) have already been paid, Part B - Fee(s) Transmittal should be completed and returned. 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.

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.

PTOL-85 (Rev. 11/03) Approved for use through 04/30/2004.

FJN 013041
SOPHOS
EXHIBIT 1004 - PAGE 0520

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 (703) 746-4000

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 4 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: Legibly mark-up with any corrections or use Block 1)

30256 7590 06/04/2004

SQUIRE, SANDERS & DEMPSEY L.L.P
600 HANSEN WAY
PALO ALTO, CA 94304-1043

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.

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, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/539,667	03/30/2000	Shlomo Touboul	40492.00011	8436

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE	PUBLICATION FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	~~YES~~ NO	~~$665~~ $1330	$0	~~$665~~ $1350	09/07/2004

EXAMINER	ART UNIT	CLASS-SUBCLASS
REVAK, CHRISTOPHER A	2131	713-181000

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.

1 _____
2 _____
3 _____

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. Inclusion of assignee data is only appropriate when an assignment has been previously submitted to the USPTO or is being submitted under separate cover. 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 enclosed:

❑ Issue Fee
❑ Publication Fee
❑ Advance Order - # of Copies _____

4b. Payment of Fee(s):

❑ A check in the amount of the fee(s) is enclosed.
❑ Payment by credit card. Form PTO-2038 is attached.
❑ The Director is hereby authorized by charge the required fee(s), or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

Director for Patents is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above.

(Authorized Signature) (Date)

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.

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, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, 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.

TRANSMIT THIS FORM WITH FEE(S)

FJN 013042
SOPHOS
EXHIBIT 1004 - PAGE 0521

Notice of Allowability	Application No.	Applicant(s)	
	09/539,667	TOUBOUL, SHLOMO	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- 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 *amendment filed February 27, 2004*.

2. ☒ The allowed claim(s) is/are *1-6,8,10-16,18,20-22*.

3. ☐ The drawings filed on _____ are accepted by the Examiner.

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 Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

FJN 013043
SOPHOS
EXHIBIT 1004 - PAGE 0522

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.
09/539,667	03/30/2000	Shlomo Touboul	40492.00011	8436

30256 7590 06/04/2004

SQUIRE, SANDERS & DEMPSEY L.L.P
600 HANSEN WAY
PALO ALTO, CA 94304-1043

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	12

DATE MAILED: 06/04/2004

Determination of Patent Term Extension under 35 U.S.C. 154 (b)
(application filed after June 7, 1995 but prior to May 29, 2000)

The Patent Term Extension is 0 day(s). Any patent to issue from the above-identified application will include an indication of the 0 day extension on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Extension is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) system (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (703) 305-1383. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (703) 305-8283.

PTOL-85 (Rev. 11/03) Approved for use through 04/30/2004.

FJN 013044
SOPHOS
EXHIBIT 1004 - PAGE 0523

DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Marc Sockol on May 13, 2004.

The application has been amended as follows:

On page 1 of the specification, line 7, after –November 6, 1997,--, please insert "which is now U.S. Patent 6,092,194,";

On page 1 of the specification, line 15, after –January 29, 1997,--, please insert " which is now U.S. Patent 6,167,520,";

In claim 1, on line 8, please insert "hashing" before –function--;

Please cancel claim 7;

In claim 8, line 2, after –fetching--, please delete –the-- and insert "a";

In claim 11, lines 6-7, please delete –for fetching-- and insert "that fetches" and on line 8, please insert "hashing" before –function--;

Please cancel claim 17;

In claim 18, line 2, after –fetches--, please delete –the-- and insert "a";

In claim 21, on line 7, please insert "hashing" before –function--;

In claim 22, on line 7, please insert "hashing" before –function--;

Allowable Subject Matter

2. The following is an examiner's statement of reasons for allowance:

It was not found to be taught in the art of a downloadable that includes references to software components required to be executed by the downloadable and performing a hashing function on the downloadable and the fetched software component to generate a downloadable ID.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 703-305-1843. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

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).

CR

May 13, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Notice of References Cited	Application/Control No. 09/539,667	Applicant(s)/Patent Under Reexamination TOUBOUL, SHLOMO	
	Examiner Christopher A. Revak	Art Unit 2131	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,339,829 B1	01-2002	Beadle et al.	713/201
	B	US-5,832,274 A	11-1998	Cutler et al.	717/171
	C	US-5,579,509 A	11-1996	Furtney et al.	703/27
	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	1132796 A1	09-2001	EP	Mas Ribes	G06F 1/00
	O	1091276 A1	04-2001	EP	Brette	G06F 1/00
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Schmitt, ".EXE. files, OS-2 style" November 1988, PC Tech Journal via dialog search, Vol. 6, #11, pg 76-78
	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.

Date Mailed: February 25, 2004	By: MAS/say	PTO DATE STAMP:
Serial No.: 09/539,667		Docket No.: 43426.00011
Applicant(s): Shlomo Touboul		

Title: SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

The following has been received in the U.S. Patent Office on the date stamped hereon:

- ☐ Patent Application __ Pages __ Claims
- ☐ Drawing Formal ___ Sheet
- ☐ General Authorization / Request to Petition for Extensions of Time
- ☐ Oath/Declaration/Power of Attorney (signed)
- ☐ Assignment & Recordation Cover Sheet
- ☐ Verified Statement Claiming Small Entity Status
- ☐ Continued Prosecution Application (§1.53(d)
- ☐ Provisional Application _____ Pages
- ☐ Design Application __ Pages __ Drawings
- ☒ Request for Continued Examination (RCE) Transmittal (1 page)
- ☒ Certificate(s) of First Class Mailing
- ☒ Amendment and Response (6 pages)
- ☒ Petition for Extension of Time (in duplicate)
- ☒ Transmittal Form
- ☒ Fee Transmittal for FY 2004 (in duplicate)
- ☐ Appeal Brief (in triplicate)
- ☐ Petition for Extension of Time (in duplicate)
- ☐ Copy of PTO-1533, Notice to File Missing Parts
- ☐ Info. Disclosure Statement & PTO-1449/Refs ____
- ☐ Other:

U.S DEPARTMENT OF COMMERCE
PATENT/TRADEMARK OFFICE
WASHINGTON, D.C. 20231

Squire, Sanders & Dempsey L.L.P.
600 Hansen Way
Palo Alto, CA 94304-1043

PTO/SB/21 (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
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.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Art Unit	2131
Examiner Name	Revak, Christopher A.
Total Number of Pages in This Submission: 12	Attorney Docket Number: 43426.00011

ENCLOSURES *(check all that apply)*

- ☒ Fee Transmittal Form (in duplicate)
- ☐ Fee Attached
- ☒ Amendment and Response (6 pgs)
- ☐ After Final
- ☒ with RCE
- ☒ Extension of Time Request (in duplicate)
- ☒ Return Postcard
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
- ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance Communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Request for Status of Application
- ☐ Other Enclosure(s) *(please identify below)*:

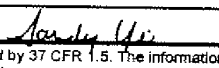
Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Marc A. Sockol, Reg. No. 40,823 Squire, Sanders & Dempsey L.L.P. 600 Hansen Way Palo Alto, CA 94304-1043
Signature	
Date	February 25, 2004

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Sandy Yi		
Signature		Date	February 25, 2004

This collection of information is required by 37 CFR 1.5. 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 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.

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
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.

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 880

Complete if Known	
Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Examiner Name	Revak, Christopher A.
Art Unit	2131
Attorney Docket No.	43426.00011

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 05-0150

Deposit Account Name: Squire, Sanders & Dempsey L.L.P.

The Director is authorized to: *(check all that apply)*
☒ Charge fee(s) indicated below ☒ Credit any overpayments
☒ Charge any additional fee(s) during the pendency of this application
☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

			Extra Claims		Fee from below		Fee Paid
Total Claims	20	-22 **	= 0	X		=	0
Independent Claims	4	-4 **	= 0	X		=	0
Multiple Dependent				X		=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	110
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive – unavoidable	
1453	1,330	2453	665	Petition to revive – unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17 (q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	770
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid SUBTOTAL (3) ($) 880

SUBMITTED BY

					Complete *(if applicable)*
Name (Print/Type)	Marc A. Sockol	*Registration No. (Attorney/Agent)*	40,823	*Telephone*	650.856.6500
Signature				*Date*	February 25, 2004

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.

This collection of information is required by 37 CFR 1.17 and 1.27. 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 this form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

COPY

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
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.

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 880

Complete if Known	
Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Examiner Name	Revak, Christopher A.
Art Unit	2131
Attorney Docket No.	43426.00011

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 05-0150

Deposit Account Name: Squire, Sanders & Dempsey L.L.P.

The Director is authorized to: *(check all that apply)*
☒ Charge fee(s) indicated below ☒ Credit any overpayments
☒ Charge any additional fee(s) during the pendency of this application
☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

			Extra Claims		Fee from below	=	Fee Paid
Total Claims	20	-22 **	= 0	X		=	0
Independent Claims	4	-4 **	= 0	X		=	0
Multiple Dependent				X		=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	110
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive – unavoidable	
1453	1,330	2453	665	Petition to revive – unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17 (q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	770
1802	900	1802	900	Request for expedited examination of a design application	
Other fee (specify) ____					

*Reduced by Basic Filing Fee Paid SUBTOTAL (3) ($) 880

SUBMITTED BY (Complete *(if applicable)*)

Name (Print/Type)	Marc A. Sockol	*Registration No. (Attorney/Agent)*	40,823	*Telephone*	650.856.6500
Signature				*Date*	February 25, 2004

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.

This collection of information is required by 37 CFR 1.17 and 1.27. 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 this form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/22 (08-03)
Approved for use through 7/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 43426.00011

In re Application of Shlomo Touboul	
Application Number 09/539,667	Filed March 30, 2000
For SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES	
Art Unit 2131	Examiner Revak, Christopher A.

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 appropriate non-small-entity fee are as follows (check time period desired):

- ☒ One month (37 CFR 1.17(a)(1)) $110.00
- ☐ Two months (37 CFR 1.17(a)(2)) $____
- ☐ Three months (37 CFR 1.17(a)(3)) $____
- ☐ Four months (37 CFR 1.17(a)(4)) $____
- ☐ Five months (37 CFR 1.17(a)(5)) $____

☐ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee amount shown above is reduced by one-half, and the resulting fee is: $ ____ .

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

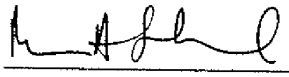
☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 05-0150 .
I have enclosed a duplicate copy of this sheet.

I am the
- ☐ applicant/inventor.
- ☐ 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).
- ☒ attorney or agent of record. Registration Number 40,823
- ☐ attorney or agent under 37 CFR 1.34(a).
  Registration number if acting under 37 CFR 1.34(a). ____ .

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.

February 25, 2004
Date


Signature

650-843-3392
Telephone Number

Marc A. Sockol
Typed or printed name

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 1 form is 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 1.14. 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.

COPY

PTO/SB/22 (08-03)
Approved for use through 7/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 43426.00011

In re Application of Shlomo Touboul	
Application Number 09/539,667	Filed March 30, 2000
For SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES	
Art Unit 2131	Examiner Revak, Christopher A.

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 appropriate non-small-entity fee are as follows (check time period desired):

- ☒ One month (37 CFR 1.17(a)(1)) $110.00
- ☐ Two months (37 CFR 1.17(a)(2)) $_____
- ☐ Three months (37 CFR 1.17(a)(3)) $_____
- ☐ Four months (37 CFR 1.17(a)(4)) $_____
- ☐ Five months (37 CFR 1.17(a)(5)) $_____

☐ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee amount shown above is reduced by one-half, and the resulting fee is: $ _____ .

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

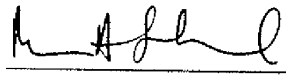
☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 05-0150 .
I have enclosed a duplicate copy of this sheet.

I am the
- ☐ applicant/inventor.
- ☐ 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).
- ☒ attorney or agent of record. Registration Number 40,823
- ☐ attorney or agent under 37 CFR 1.34(a).
  Registration number if acting under 37 CFR 1.34(a). _____ .

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.

February 25, 2004
Date

650-843-3392
Telephone Number


Signature

Marc A. Sockol
Typed or printed name

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 1 form is 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 1.14. 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.

PTO/SB/30 (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
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.

Request For Continued Examination (RCE) Transmittal

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

Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Art Unit	2131
Examiner Name	Revak, Christopher A.
Attorney Docket Number	43426.00011

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 C.F.R. 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 C.F.R. 1.103(c) for a period of _____months. (Period of suspension shall not exceed 3 months; Fee under 37 C.F.R. 1.17(i) **required**)

b. ☐ Other _____

3. Fees The RCE fee under 37 C.F.R. 1.17(e) is required by 37 C.F.R. 1.114 when the RCE is filed.

a. ☒ The Director is hereby authorized to charge the following fees, or credit any overpayments, to Deposit Account No. 05-0150
   i. ☒ RCE fee required under 37 C.F.R. 1.17(e)
   ii. ☒ Extension of time fee (37 C.F.R. 1.136 and 1.17)
   iii. ☐ Other _____

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

Name (Print /Type)	Marc A. Sockol	*Registration No. (Attorney/Agent)*	40,823
Signature		*Date*	February 25, 2004

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:

Name (Print /Type)	Sandy Yi		
Signature		*Date*	February 25, 2004

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 1.14. 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.

Attorney's Docket No.: 43426.00011

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below 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, on

Date: 2/25/2004 By: Sandy Yi
Sandy Yi

In Re Patent Application of: Shlomo Touboul	Examiner: Christopher A. Revak
Application No: 09/539,667	Art Unit: 2131
Filed: March 30, 2000	
For: SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES	

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

AMENDMENT AND RESPONSE WITH RCE

Sir:

In response to the Office Action dated October 27, 2003, the shortened statutory deadline for response ending on February 27, 2004 with the enclosed request for one-month extension and RCE, applicant respectfully requests that the above-identified application be amended as follows:

IN THE CLAIMS:

Please substitute the following claims for the pending claims with the same number:

1. (Currently amended) A computer-based method for generating a Downloadable ID to identify a Downloadable, comprising:

obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;

fetching at least one software component identified by the one or more references; and

performing a function on the Downloadable and the fetched software components to generate a Downloadable ID.

2. (Original) The method of claim 1, wherein the Downloadable includes an applet.

3. (Previously amended) The method of claim 1, wherein the Downloadable includes an active software control.

4. (Original) The method of claim 1, wherein the Downloadable includes a plugin.

5. (Original) The method of claim 1, wherein the Downloadable includes HTML code.

6. (Original) The method of claim 1, wherein the Downloadable includes an application program.

7. (Original) The method of claim 1, wherein the function includes a hashing function.

8. (Previously amended) The method of claim 1, wherein said fetching includes fetching the first software component referenced by the Downloadable.

9. (Cancelled)

10. (Previously amended) The method of claim 1, wherein said fetching includes fetching all software components referenced by the Downloadable.

11. (Currently amended) A system for generating a Downloadable ID to identify a Downloadable, comprising:

a communications engine for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable; and

an ID generator coupled to the communications engine for fetching at least one software component identified by the one or more references, and for performing a function on the Downloadable and the fetched software components to generate a Downloadable ID.

12. (Original) The system of claim 11, wherein the Downloadable includes an applet.

13. (Previously amended) The system of claim 11, wherein the Downloadable includes an active software control.

14. (Original) The system of claim 11, wherein the Downloadable includes a plugin.

15. (Original) The system of claim 11, wherein the Downloadable includes HTML code.

16. (Original) The system of claim 11, wherein the Downloadable includes an application program.

17. (Original) The system of claim 11, wherein the function includes a hashing function.

18. (Previously amended) The system of claim 11, wherein the ID generator fetches the first software component referenced by the Downloadable.

19. (Cancelled)

20. (Previously amended) The method of claim 11, wherein the ID generator fetches all software components referenced by the Downloadable.

21. (Currently amended) A system for generating a Downloadable ID to identify a Downloadable, comprising:

means for obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;

means for fetching at least one software component identified by the one or more references; and

means for performing a function on the Downloadable and the fetched software components to generate a Downloadable ID.

22. (Currently amended) A computer-readable storage medium storing program code for causing a computer to perform the steps of:

obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;

fetching at least one software component identified by the one or more references; and

performing a function on the Downloadable and the fetched software components to generate a Downloadable ID.

REMARKS

Claims 1 – 8, 10 – 18 and 20 – 22 are presented for examination. Claims 1, 11, 21 and 22 are being amended. Applicant respectfully requests reconsideration of the application in view of the amendments above and remarks below.

Applicant would like to thank the Examiner for the interview on January 27, 2004 to discuss the office action, the Apperson reference and the current claim set. During the interview, Applicant and the Examiner discussed how the system described in the Apperson reference associates privileges to a Downloadable and then allows the Downloadable to execute only those operations allowed by the associated privileges. Applicant and the Examiner discussed how the privileges in Apperson are monitored by the browser, not executed by the Downloadable, and further how the Apperson reference does not generate Downloadable IDs based on the fetched executable components. Further, Applicant and the Examiner discussed adding the language "to be executed" into the claim language to further show that the additional components are "to be executed," thereby highlighting that difference between the Apperson reference and claimed invention.

Specifically, in paragraphs 1 and 2 of the office action, the Examiner rejected claims 1, 5-8, 10, 11, 15-18 and 20-22 under 35 USC § 103(a) over Apperson. Apperson describes the use of digital certificates to authorize privileges for executable code. Such privileges include file I/O privileges, network privileges and registry privileges (Apperson / col. 2, lines 41 – 53; col. 4, lines 33 – 43; FIG. 2).

Apperson, however, does not teach fetching at least one software component referenced by a Downloadable, where the software component is "required to be executed by the Downloadable" and "performing a function on the Downloadable and the fetched software components to generate a Downloadable ID" as recited in independent claims 1, 11, 21 and 22, as amended. As will be recognized by those skilled in the art, in some embodiments, the Downloadable ID may be used to recognize the "same" Downloadable regardless of how the Downloadable is subdivided and/or downloaded before and/or during execution. Since all other claims depend from these independent claims, Applicant

FJN 013060
SOPHOS
EXHIBIT 1004 - PAGE 0539

respectfully submits that they are distinguishable over Apperson for at least the same reasons.

In paragraph 3, the Examiner rejected claims 2-4 and 12-14 over Apperson in view of Khare. Khare describes Microsoft Corporation's implementation of digital signatures, referred to as Authenticode, as applied to ActiveX controls and Java applets. Like Apperson, Khare does not teach fetching at least one software component referenced by a Downloadable, where the software component is "required to be executed by the Downloadable" and "performing a function on the Downloadable and the fetched software components to generate a Downloadable ID" as recited in independent claims 1, 11, 21 and 22, as amended. Since claims 2-4 and 12-14 depend from claims 1 and 11, respectively, Applicant respectfully submits that they are patentable for at least the same reasons.

For the foregoing reasons, applicant respectfully submits that the claims are in condition for allowance.

If the Examiner has any questions or needs any additional information, the Examiner is invited to telephone the undersigned attorney at (650) 843-3392. If for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No. 05-0150.

Date: February 25, 2004

Respectfully submitted,

Squire, Sanders & Dempsey L.L.P.
600 Hansen Way
Palo Alto, CA 94304-1043
Telephone: (650) 856-6500
Facsimile: (650) 843-8777

By: _____
Marc A. Sockol
Attorney for Applicant
Registration No. 40,823

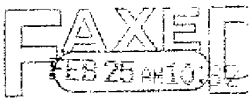
FJN 013061
SOPHOS
EXHIBIT 1004 - PAGE 0540

SQUIRE SANDERS | LEGAL COUNSEL WORLDWIDE

SQUIRE, SANDERS & DEMPSEY L.L.P.

600 Hansen Way
Palo Alto, CA 94304-1043
Office: +1.650.856.6500
Fax: +1.650.843.8777

Preferred Fax: ___
If Problems: ___



February 25, 2004

PLEASE DELIVER THESE PAGES IMMEDIATELY

Number Of Pages (including cover): 7

TO:	Examiner Chris Revak	**FAX NO.:**	703-746-7622
COMPANY:	U.S. Patent and Trademark Office	**PHONE NO.:**	703-305-1843
FROM:	Marc A. Sockol	**DIRECT DIAL NO.:**	+1.650.843.3392
E-MAIL:	MSockol@ssd.com		

RE: U.S. Patent Application
Entitled: "System and Method for Protecting a Computer and a Network from Hostile Downloadables"
Serial No.: 09/539,667
Inventor: Shlomo Touboul
Filing Date: March 30, 2000
Our Ref.: 43426.00011

Dear Chris,

Attached please find a courtesy copy of the Amendment and Response with RCE which we filed via U.S. mail today. If you have any questions, please contact me at 650-843-3392. Thank you for your time and consideration.

Sincerely,

Marc

CONFIDENTIALITY NOTICE:
The attached information is LEGALLY PRIVILEGED AND CONFIDENTIAL and is intended only for the use of the addressee named above. If the reader of this message is not the intended recipient or the employee or agent responsible for delivering the message to the intended recipient, please be aware that any dissemination, distribution or duplication of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and return the original message to us at the address above via the postal service. Thank you.

Sender No.:	11585	43426.00011	Sandy Yi
Job No:		Account No.	Return to Office

* * * COMMUNICATION RESULT REPORT (FEB.25.2004 11:23AM) * * *

FAX HEADER: SQUIRE SANDERS

FILE MODE	OPTION	ADDRESS (GROUP)	RESULT	PAGE
520 MEMORY TX		917037467622	OK	P. 7/7

REASON FOR ERROR
E-1) HANG UP OR LINE FAIL
E-2) BUSY
E-3) NO ANSWER
E-4) NO FACSIMILE CONNECTION

SQUIRE SANDERS | LEGAL COUNSEL WORLDWIDE

SQUIRE, SANDERS & DEMPSEY L.L.P.

600 Hansen Way
Palo Alto, CA 94304-1043
Office: +1.650.856.6500
Fax: +1.650.843.8777

Preferred Fax: ___
If Problems: ___

February 25, 2004

PLEASE DELIVER THESE PAGES IMMEDIATELY

Number Of Pages (including cover): 7

TO: Examiner Chris Revak **FAX NO.:** 703-746-7622

COMPANY: U.S. Patent and Trademark Office **PHONE NO.:** 703-305-1843

FROM: Marc A. Sockol **DIRECT DIAL NO.:** +1.650.843.3392

E-MAIL: MSockol@ssd.com

RE: **U.S. Patent Application**
Entitled: **"System and Method for Protecting a Computer and a Network from Hostile Downloadables"**
Serial No.: **09/539,667**
Inventor: **Shlomo Touboul**
Filing Date: **March 30, 2000**

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.
09/539,667	03/30/2000	Shlomo Touboul	~~40492.00011~~ 43426	8436

30256 7590 10/27/2003

SQUIRE, SANDERS & DEMPSEY L.L.P
600 HANSEN WAY
PALO ALTO, CA 94304-1043

EXAMINER	
REVAK, CHRISTOPHER A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/27/2003

Response to FINAL OA Due: 1/27/04
Notice of Appeal: 4/27/04

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

DATES ENTERED
Response Due
1/27/04

OCT 30 2003

CALENDARED
BY SAY
ATTORNEY
SQUIRE, SANDERS & DEMPSEY

PTO-90C (Rev. 10/03)

Office Action Summary	Application No.	Applicant(s)	
	09/539,667	TOUBOUL, SHLOMO	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- 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) 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 the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- 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 August 2003* .

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) *1-8,10-18 and 20-22* 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) *1-8,10-18,20-22* 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 _____ 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).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ 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.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

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-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

1.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed on August 4, 2003 have been fully considered but they are not persuasive. The examiner notes the applicant's arguments pertaining to Apperson et al failing to recite of "obtaining one or more references to software components required by the downloadable" and "performing a function on the downloadable and the fetched software components to generate a downloadable ID," however the examiner has not been persuaded by the applicant's remarks. As support of the examiner's stance taken on it being obvious for "executable code (downloadable) includes any references", the examiner has provided the teachings of Doyle et al as support for the stance taken. Doyle et al recites of dynamic link libraries allow executables (downloadables) to be stored separately with as files with calling extensions and to be loaded only when needed by the program (pg 137-138). Although Doyle et al discloses of the storing the dlls separately, they access functions (obtaining one or more references on the downloadable) for the executable. Furthermore, the use of dynamic link libraries are associated with the executable file the teachings of Apperson et al perform the function of a SHA-hash (function) on the executable code (col. 4, lines 44-48) that includes the dynamic link library.

Claim Rejections - 35 USC § 103

I. 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 negatived by the manner in which the invention was made.

II. Claims 1,5-8,10,11,15-18,20,21, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Apperson et al.

As per claims 1,11,21, and 22, Apperson et al discloses of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege categories that the executable code (downloadable) may try to perform on the client machine (one or more references to a component). The distributing authority digitally signs (performs a function) the executable code and the privilege request code and provides a certificate (generated downloadable ID) that can be traced by a client to a known certifying authority (col. 2, lines 43-53). Also recited by Apperson et al of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege categories (first and all components referenced) that the executable code (downloadable) may try to perform on the client machine (one or more references to a component)(col. 2, lines 43-47). The teachings of Apperson et al are silent in disclosing that the executable code (downloadable) does not include any references. The examiner hereby asserts that it is obvious for the teachings of Apperson et al to make use of this feature. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to include or exclude components in executable code (downloadable). The governing factor would be the intent of the executable code (downloadable) and

how it was designed. If it were a independent of any other function within an interactive environment, such as documents on the World Wide Web, then it could be executed independent of any other components once downloaded onto a user's computer. Otherwise, if downloaded executable code was dependent on functions on a user's computer as is explicitly disclosed by Apperson et al (col. 2, lines 43-47), then the specific functions would be referenced by the executable code (downloadable). It is obvious that the teachings of Apperson et al could have include executable code (downloadable) without including any references since there exists various types of executable code that may or may not reference other components.

As per claims 5,6,15, and 16, it is disclosed by Apperson et al of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege categories that the executable code (downloadable) may try to perform on the client machine (one or more references to a component). The distributing authority digitally signs (performs a function) the executable code and the privilege request code and provides a certificate (generated downloadable ID) that can be traced by a client to a known certifying authority (col. 2, lines 43-53). The teachings of Apperson et al disclose of digitally signing executable code (downloadables), but do not identify that the executable code (downloadable) contains specific privilege request code such as including HTML code or an application program. The examiner hereby takes official notice that it is notoriously well known that HTML code and application programs include executable code. It would have been obvious to a person of ordinary skill in the art to have been motivated to interpret the teachings of Apperson et al to have included the use of HTML code and application programs as specific forms of executable code. It is notoriously well known that HTML code and application programs are information that is transferred across the Internet and downloaded by a client

computer's browser which reads and executes the executable code. An application program is known as being a program in assisting in the performance of a specific task, namely a web based document processing and HTML is known as a markup language used for documents on the World Wide Web and indicates how web browsers should display the elements of a web document to a user. It is obvious that the teachings of Apperson et al could have included HTML code and application code as forms of executable code (downloadables) since it is executable information which is transferred across the Internet.

As per claims 7 and 17, Apperson et al discloses of performing the function of a SHA-hash (function) on the executable code (col. 4, lines 44-48).

As per claims 8,10,18, and 20, it is taught by Apperson et al of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege categories (first and all components referenced) that the executable code (downloadable) may try to perform on the client machine (col. 2, lines 43-47).

III. Claims 2-4 and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Apperson et al in view of Khare.

It is disclosed by Apperson et al of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege categories that the executable code (downloadable) may try to perform on the client machine (one or more references to a component). The distributing authority digitally signs (performs a function) the executable code and the privilege request code and provides a certificate (generated downloadable ID) that can be traced by a client to a

known certifying authority (col. 2, lines 43-53). The teachings of Apperson et al disclose of digitally signing executable code (downloadables), but do not identify that the executable code (downloadable) contains specific privilege request code such as being an applet, active software control, or a plug-in. It is disclosed by Khare of an identical teaching which discloses Microsoft announcing a tool that allows vendors to digitally sign active software controls, Java (applets), and plug-in components (pg 1). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply code signing to information such as active software controls, Java applets, and plug-in components. The teachings of Khare disclose that the intent of code signing is to identify a creator of an Internet based applet before a user downloads it and it is designed to provide users with the same level of security found in marketed software which is based on a level of trust and place pressure on independent service vendors (ISVs) honest and the additionally issue digital certificates to the executables (downloadable) components such as ActiveX (active software) controls (pg 1). Apperson et al additional recites of motivation that enables servers to download executables (downloadables) with full client validation of their origin and authenticity (col. 2, lines 34-38) and the teachings of Khare are an obvious extension of the teachings of Apperson et al as a means of identifying specific components such as an applet, active software control, or a plug-in to provide a user/client with information about the executable (downloadable) and if it is trusted from an external source and if it has been authenticated.

Conclusion

IV. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

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.

V. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Doyle et al, "Microsoft Press Computer Dictionary"

VI. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher Revak whose telephone number is (703) 305-1843. The examiner can normally be reached on Monday-Thursday from 6:30 am to 4:00 pm. The examiner can also be reached on alternate Fridays from 6:30 am to 3:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned as follows:

for After-Final Communications: (703) 746-7238;

for Official Communications: (703) 746-7239;

for Non-Official Communications: (703) 746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

CR
October 13, 2003

FRANTZ B. JEAN
PRIMARY EXAMINER

Notice of References Cited	Application/Control No. 09/539,667	Applicant(s)/Patent Under Reexamination TOUBOUL, SHLOMO	
	Examiner Christopher A. Revak	Art Unit 2131	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	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

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Doyle et al, "Microsoft Press Computer Dictionary" 1993, Microsoft Press, 2nd Edition, pg 137-138
	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.

Date Mailed: July 31, 2003	By: MAS/emj	PTO DATE STAMP:
Application No.: 09/539,667		Docket No.: 43426.00011
Applicant: Shlomo Touboul		
Title: SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES		

The following has been received in the U.S. Patent Office on the date stamped hereon:

- ☐ Patent Application __ Pages __ Claims
- ☐ Drawings Informal ___ Sheets
- ☐ General Authorization / Request to Petition for Extensions of Time
- ☐ Oath/Declaration
- ☐ Assignment & Recordation Cover Sheet
- ☐ Verified Statement Claiming Small Entity Status
- ☐ Continued Prosecution Application (§1.53(d)
- ☐ Provisional Application _____ Pages
- ☐ Design Application __ Pages __ Drawings
- ☐ Status Letter
- ☐ Check No. for $
- ☐ Power of Attorney
- ☒ Certificate(s) of First Class Mailing
- ☒ Response/Amendment
- ☐ Petition for Extension of Time
- ☒ Transmittal Form
- ☐ Notice of Appeal
- ☒ Fee Transmittal (in duplicate)
- ☐ Issue Fee Transmittal with PTO-85b
- ☐ Copy of PTO-1533; Notice to File Missing Parts
- ☐ Info. Disclosure Statement & PTO-1449/Refs ___
- ☐ Request to Correct Filing Receipt
- ☐ Check No. for $
- ☒ Other: Terminal Disclaimer

U.S DEPARTMENT OF COMMERCE
PATENT/TRADEMARK OFFICE
WASHINGTON, D.C. 20231

Squire, Sanders & Dempsey L.L.P.
600 Hansen Way, Suite 100
Palo Alto, CA 94304-1043

PTO/SB/21 (05-03)
Approved for use through 04/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
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.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Art Unit	2131
Examiner Name	Christopher A. Revak
Total Number of Pages in This Submission	13
Attorney Docket Number	43426.00011

ENCLOSURES *(check all that apply)*

- ☒ Fee Transmittal Form
- ☐ Request for Corrected Filing Receipt
- ☒ Amendment / Response
  - ☐ After Final
  - ☐ With RCE
- ☐ Extension of Time Request
- ☒ Return Postcard
- ☐ IDS and Form 1449
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
- ☐ Declaration/Oath
- ☐ Assignment and Recordation Cover Sheet *(for an Application)*
- ☐ Drawing(s) ____ Sheets
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ RCE
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☒ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) ____
- ☐ After Allowance Communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
- ☐ Proprietary Information
- ☐ Status Request
- ☐ Other Enclosure(s) *(please identify below):*

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Marc A. Sockol, Reg. No. 40,823 Squire, Sanders & Dempsey, L.L.P. 600 Hansen Way Palo Alto, CA 94304-1043
Signature	
Date	July 31, 2003

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Eileen M. Janikowski		
Signature		Date	July 31, 2003

This collection of information is required by 37 CFR 1.5. 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 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.

PTO/SB/17 (05-03)
Approved for use through 04/30/2003. OMB 0651-0032
U.S. Patent a... demark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Red... Act of 1995, no persons are required to respond to a collection of i... ation unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2003

Effective 01/01/2003. Patent fees are subject to annual revision.

☒ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 110

Complete if Known	
Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Examiner Name	Christopher A. Revak
Art Unit	2131
Attorney Docket No.	43426.00011

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 05-0150

Deposit Account Name: Squire, Sanders & Dempsey, L.L.P.

The Director is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s) during the pendency of this application

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	750	2001	375	Utility filing fee	
1002	330	2002	165	Design filing fee	
1003	520	2003	260	Plant filing fee	
1004	750	2004	375	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below		Fee Paid
Total Claims		-20 **	= 0	X		=	0
Independent Claims		-3 **	= 0	X		=	0
Multiple Dependent				X		=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	84	2201	42	Independent claims in excess of 3
1203	280	2203	140	Multiple dependent claim, if not paid
1204	84	2204	42	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

***or number previously paid, if greater; For Reissues, see above*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	410	2252	205	Extension for reply within second month	
1253	930	2253	465	Extension for reply within third month	
1254	1,450	2254	725	Extension for reply within fourth month	
1255	1,970	2255	985	Extension for reply within fifth month	
1401	320	2401	160	Notice of Appeal	
1402	320	2402	160	Filing a brief in support of an appeal	
1403	280	2403	140	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive – unavoidable	
1453	1,300	2453	650	Petition to revive – unintentional	
1501	1,300	2501	650	Utility issue fee (or reissue)	
1502	470	2502	235	Design issue fee	
1503	630	2503	315	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17 (q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	750	2809	375	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	750	2810	375	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	750	2801	375	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) Terminal Disclaimer Fee: 110

*Reduced by Basic Filing Fee Paid SUBTOTAL (3) ($) 110

SUBMITTED BY				Complete *(if applicable)*	
Name (Print/Type)	Marc A. Sockol	*Registration No. Attorney/Agent)*	40,823	*Telephone*	(650) 856-6500
Signature				*Date*	July 31, 2003

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.

This collection of information is required by 37 CFR 1.17 and 1.27. 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 this form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

COPY

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

U.S. Patent a... demark Office: U.S. DEPARTMENT OF COMMERCE

Approved for use through 04/30/2003. OMB 0651-0032

(PTO/SB/17 (12-02-03)

COPY

FEE TRANSMITTAL for FY 2003

Effective 01/01/2003. Patent fees are subject to annual revision.

☒ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 110

Complete If Known	
Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Examiner Name	Christopher A. Revak
Art Unit	2131
Attorney Docket No.	43426.00011

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 05-0150

Deposit Account Name: Squire, Sanders & Dempsey, L.L.P.

The Director is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s) during the pendency of this application

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	750	2001	375	Utility filing fee	
1002	330	2002	165	Design filing fee	
1003	520	2003	260	Plant filing fee	
1004	750	2004	375	Reissue filing fee	
1005	160	2005	80	Provisional filling fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below		Fee Paid
Total Claims		-20 **	= 0	X		=	0
Independent Claims		-3 **	= 0	X		=	0
Multiple Dependent				X		=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	84	2201	42	Independent claims in excess of 3
1203	280	2203	140	Multiple dependent claim, if not paid
1204	84	2204	42	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

***or number previously paid, if greater; For Reissues, see above*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	410	2252	205	Extension for reply within second month	
1253	930	2253	465	Extension for reply within third month	
1254	1,450	2254	725	Extension for reply within fourth month	
1255	1,970	2255	985	Extension for reply within fifth month	
1401	320	2401	160	Notice of Appeal	
1402	320	2402	160	Filing a brief in support of an appeal	
1403	280	2403	140	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive – unavoidable	
1453	1,300	2453	650	Petition to revive – unintentional	
1501	1,300	2501	650	Utility issue fee (or reissue)	
1502	470	2502	235	Design issue fee	
1503	630	2503	315	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17 (q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	750	2809	375	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	750	2810	375	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	750	2801	375	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	
Other fee (specify) Terminal Disclaimer Fee					110

*Reduced by Basic Filing Fee Paid SUBTOTAL (3) ($) 110

SUBMITTED BY				Complete *(if applicable)*	
Name (Print/Type)	Marc A. Sockol	*Registration No. Attorney/Agent)*	40,823	*Telephone*	(650) 856-6500
Signature				*Date*	July 31, 2003

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.

This collection of information is required by 37 CFR 1.17 and 1.27. 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 this form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Attorney's Docket No.: 43426.00011 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on

Date: July 31, 2003 By: Eileen M. Janikowski

In Re Patent Application of:

Shlomo Touboul

Application No: 09/539,667

Filed: March 30, 2000

For: SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

Examiner: Christopher A. Revak

Art Unit: 2131

Assistant Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO OFFICE ACTION UNDER 37 C.F.R. §1.111

Sir:

In response to the Office Action dated July 1, 2003 and pursuant to 37 C.F.R. §1.111, applicant respectfully requests that the above-identified application be amended as follows:

IN THE ABSTRACT OF THE DISCLOSURE:

Kindly replace the Abstract of the Disclosure with the following text:

-- A computer-based method for generating a Downloadable ID to identify a Downloadable, including obtaining a Downloadable that includes one or more references to software components required by the Downloadable, fetching at least one software component identified by the one or more references, and performing a function on the Downloadable and the fetched software components to generate a Downloadable ID. A system and a computer-readable storage medium are also described and claimed. --

IN THE CLAIMS:

Kindly cancel claims 9 and 19 without prejudice.

Please substitute the following claims for the pending claims with the same number:

1. (Currently amended) A computer-based method for generating a Downloadable ID to identify a Downloadable, comprising [the steps of]:

obtaining a Downloadable that includes one or more references to software components required by the Downloadable;

fetching[, if the Downloadable includes one or more references to a component,] at least one software component identified by the one or more references; and

performing a function on the Downloadable and [all] the fetched software components [fetched] to generate a Downloadable ID.

2. (Original) The method of claim 1, wherein the Downloadable includes an applet.

3. (Currently amended) The method of claim 1, wherein the Downloadable includes an [ActiveX™] active software control.

4. (Original) The method of claim 1, wherein the Downloadable includes a plugin.

5. (Original) The method of claim 1, wherein the Downloadable includes HTML code.

6. (Original) The method of claim 1, wherein the Downloadable includes an application program.

7. (Original) The method of claim 1, wherein the function includes a hashing function.

FJN 013081
SOPHOS
EXHIBIT 1004 - PAGE 0560

8. (Currently amended) The method of claim 1, wherein [the step of] said fetching includes [the step of] fetching the first software component referenced by the Downloadable.

9. (Cancelled)

10. (Currently amended) The method of claim 1, wherein [the step of] said fetching includes fetching all software components referenced by the Downloadable.

11. (Currently amended) A system for generating a Downloadable ID to identify a Downloadable, comprising:

a communications engine for obtaining a Downloadable that includes one or more references to software components required by the Downloadable; and

an ID generator coupled to the communications engine for fetching[, if the Downloadable includes one or more references to a component,] at least one software component identified by the one or more references, and for performing a function on the Downloadable and [all] the fetched software components [fetched] to generate a Downloadable ID.

12. (Original) The system of claim 11, wherein the Downloadable includes an applet.

13. (Currently amended) The system of claim 11, wherein the Downloadable includes an [ActiveX™] active software control.

14. (Original) The system of claim 11, wherein the Downloadable includes a plugin.

15. (Original) The system of claim 11, wherein the Downloadable includes HTML code.

FJN 013082
SOPHOS
EXHIBIT 1004 - PAGE 0561

16. (Original) The system of claim 11, wherein the Downloadable includes an application program.

17. (Original) The system of claim 11, wherein the function includes a hashing function.

18. (Currently amended) The system of claim 11, wherein the ID generator fetches the first software component referenced by the Downloadable.

19. (Cancelled)

20. (Currently amended) The method of claim 11, wherein the ID generator fetches all software components referenced by the Downloadable.

21. (Currently amended) A system for generating a Downloadable ID to identify a Downloadable, comprising:

means for obtaining a Downloadable that includes one or more references to software components required by the Downloadable;

means for fetching[, if the Downloadable includes one or more references to a component,] at least one software component identified by the one or more references; and

means for performing a function on the Downloadable and [all] the fetched software components [fetched] to generate a Downloadable ID.

22. (Currently amended) A computer-readable storage medium storing program code for causing a computer to perform the steps of:

obtaining a Downloadable that includes one or more references to software components required by the Downloadable;

fetching[, if the Downloadable includes one or more references to a component,] at least one software component identified by the one or more references; and

performing a function on the Downloadable and [all] the fetched software components [fetched] to generate a Downloadable ID.

FJN 013083
SOPHOS
EXHIBIT 1004 - PAGE 0562

REMARKS

Applicant has carefully studied the outstanding Office Action. The present amendment is intended to place the application in condition for allowance and is believed to overcome all of the objections and rejections made by the Examiner. Favorable reconsideration and allowance of the application are respectfully requested.

Applicant has canceled claims 9 and 19, and amended claims 1, 3, 8, 10, 11, 13, 18 and 20 - 22 to more properly claim the present invention. No new matter has been added. Claims 1 – 8, 10 – 18 and 20 – 22 are presented for examination.

Applicant notes that the page headers of the Office Action indicate an incorrect Application/Control Number.

In paragraphs 2 and 3 of the Office Action, the Examiner has objected to the abstract of the disclosure. Accordingly, applicant has amended the abstract so as to conform to the proper language and format.

In paragraphs 4 and 5 of the Office Action, the Examiner has rejected claims 1, 11, 21 and 22 under the judicially created doctrine of double patenting. Accordingly, applicant is submitting a terminal disclaimer with the present amendment.

In paragraphs 6 and 7 of the Office Action, the Examiner has rejected claims 3 and 13 under 35 U.S.C. §112, second paragraph as being indefinite. Applicant has amended these claims accordingly.

In paragraphs 8 and 9 of the Office Action, the Examiner has rejected claims 1, 7, 8, 10, 11, 17, 18, and 20 – 22 under 35 U.S.C. §102(e) as being anticipated by Apperson et al., U.S. Patent No. 5,978,484 ("Apperson").

In paragraphs 10 and 11 of the Office Action, the Examiner has rejected claims 2 – 4 and 12 – 14 under 35 U.S.C. §103(a) as being unpatentable over Apperson in view of Khare, "*Microsoft Authenticode Analyzed*", July 22, 1996, xent.com/FoRK-archive/summer96/0338.html, pg. 1 and 2 ("Khare").

In paragraph 12 of the Office Action, the Examiner has rejected claims 5, 6, 9, 15, 16 and 19 under 35 U.S.C. §103(a) as being unpatentable over Apperson. Applicant has canceled claims 9 and 19 without acquiescence to the Examiner's reasons for rejection and respectfully submits that rejection of those claims is thus rendered moot.

FJN 013084
SOPHOS
EXHIBIT 1004 - PAGE 0563

Distinctions between Claimed Invention and U.S. Patent No. 5,978,484 to Apperson et al in view of Khare, "Microsoft Authenticode Analyzed", July 22, 1996, xent.com/FoRK-archive/summer96/0338.html, pg. 1 and 2

The present invention concerns generation of an ID for mobile code downloaded to a client computer, referred to as a Downloadable. Specifically, the present invention fetches software components required by the Downloadable, and performs a hashing function on the Downloadable together with its fetched components (original specification / page 3, lines 11 – 14; page 15, lines 21 – 24; page 19, line 21 – page 20, line 6; FIG. 8). Thus, for a Java applet, the present invention fetches Java classes identified by the applet bytecode, and generates the Downloadable ID from the applet and the fetched Java classes; and for an ActiveX™ control, the present invention fetches components listed in its .INF file, and generates a Downloadable ID from the ActiveX™ control and the fetched components (original specification / page 9, lines 15 – 18).

An advantage of the present invention is that it produces the same ID for a Downloadable, regardless of which software components are included with the Downloadable and which software components are only referenced (original specification / page 9, lines 18 – 20; page 20, lines 5 and 6). The same Downloadable may be delivered with some required software components included and others missing, and in each case the generated Downloadable ID will be the same. Thus the same Downloadable is recognized through many equivalent guises.

Apperson describes use of digital certificates to authorize privileges for executable code, such as file I/O privileges, network privileges and registry privileges (Apperson / col. 2, lines 41 – 53; col. 4, lines 33 – 43; FIG. 2).

Khare describes Microsoft Corporation's implementation of digital signatures, referred to as Authenticode, as applied to ActiveX controls and Java applets.

In distinction to the present invention, Apperson and Khare do not teach fetching software components of executable code. In order to further clarify this distinction, applicant has amended the claims so as to refer to software components required by the Downloadable.

In paragraph 9 of the Office Action, the Examiner has indicated that Apperson discloses fetching components of a Downloadable. Applicant respectfully submits that Apperson's privilege request code does not include components of a Downloadable, but instead includes a list of "*privileges or*

FJN 013085
SOPHOS
EXHIBIT 1004 - PAGE 0564

privilege categories that the executable code might perform on the client machine" (Apperson / col. 2, lines 45 – 47).

The rejections of claims 1 –8 and 10 in paragraphs 8 - 12 of the Office Action will now be dealt with specifically.

As to amended independent method claim 1, applicant respectfully submits that the limitation in claim 1 of:

"*fetching at least one software component identified by the one or more references*"

is neither shown nor suggested in Apperson or Khare.

Because claims 2 – 8 and 10 depend from claim 1 and include additional features, applicant respectfully submits that claims 2 - 8 and 10 are not anticipated or rendered obvious by Apperson and Khare, taken alone or in combination.

Accordingly claims 1 – 8 and 10 are deemed to be allowable.

As to amended independent system claim 11, applicant respectfully submits that the limitation in claim 11 of:

"*an ID generator coupled to the communications engine for fetching at least one software component identified by the one or more references*"

is neither shown nor suggested in Apperson or Khare.

Because claims 12 – 18 and 20 depend from claim 11 and include additional features, applicant respectfully submits that claims 12 – 18 and 20 are not anticipated or rendered obvious by Apperson and Khare, taken alone or in combination.

Accordingly claims 12 – 18 and 20 are deemed to be allowable.

As to amended independent system claim 21, applicant respectfully submits that the limitation in claim 21 of:

"*means for fetching at least one software component identified by the one or more references*"

is neither shown nor suggested in Apperson or Khare.

Accordingly claim 21 is deemed to be allowable.

As to amended independent system claim 22, applicant respectfully submits that the limitation in claim 22 of:

"*fetching at least one software component identified by the one or more references*"

is neither shown nor suggested in Apperson or Khare.

Accordingly claim 22 is deemed to be allowable.

FJN 013086
SOPHOS
EXHIBIT 1004 - PAGE 0565

Support for Amended Claims in Original Specification

Regarding amended claims 1, 8, 10, 11, 18 and 20 - 22, fetching software components is described in the original specification on page 9, lines 13 – 18 and FIG. 8.

For the foregoing reasons, applicant respectfully submits that the applicable objections and rejections have been overcome and that the claims are in condition for allowance.

If the Examiner has any questions or needs any additional information, the Examiner is invited to telephone the undersigned attorney at (650) 843-3392. If for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No. 05-0150.

Date: July 31, 2003

Respectfully submitted,

Squire, Sanders & Dempsey L.L.P.
600 Hansen Way
Palo Alto, CA 94304-1043
Telephone: (650) 856-6500
Facsimile: (650) 843-8777

By: _____
Marc A. Sockol
Attorney for Applicant
Registration No. 40,823

FJN 013087
SOPHOS
EXHIBIT 1004 - PAGE 0566

PTO/ SB/26 (05-03)
Approved for use through 4/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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	Docket Number (Optional) 43426.00011

In re Application of: Shlomo Touboul

Application No. 09/539,667

Filed: March 30, 2000

For: SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADING

The owner*, Finjan Software, Ltd. 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 defined in 35 U.S.C. 154 and 173, as presently shortened by any terminal disclaimer, of prior Patent No. 6,092,194. 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.

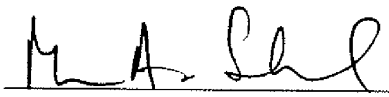
In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the prior patent, as presently shortened by any terminal disclaimer, in the event that it 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 cancelled 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 an organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the 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 of record.



July 31, 2003

Signature Date

Marc A. Sockol, Reg. No. 40,823

Typed or printed name

(650) 856-6500

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.

*Certification 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 1.14. 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, VA22313-1450.**

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.
09/539,667	03/30/2000	Shlomo Touboul	~~40492~~.00011 42426	8436

30256 7590 07/01/2003

SQUIRE, SANDERS & DEMPSEY L.L.P
600 HANSEN WAY
PALO ALTO, CA 94304-1043

EXAMINER	
REVAK, CHRISTOPHER A	

ART UNIT	PAPER NUMBER
2131	5

DATE MAILED: 07/01/2003

Response Due: 10/1/2003
FINAL: 1/1/2004

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

DATES ENTERED
Response Due 10/1/2003

JUL 07 2003

CALENDARED
BY _____
ATTORNEY
SQUIRE, SANDERS & DEMPSEY

PTO-90C (Rev. 07-01)

Office Action Summary	Application No.	Applicant(s)	
	09/539,667	TOUBOUL, SHLOMO	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- 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) 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 the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- 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 _____ .

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) 1-22 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) 1-22 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 _____ 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).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ 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.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

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-1449) Paper No(s) 2 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement submitted is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

2. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally ***limited to a single paragraph*** on a separate sheet within the range of 50 to 250 words. It is important that the abstract not exceed 250 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

It is noted by the examiner that the abstract should be amended to be incorporated into a single paragraph.

3. The specification is objected to because the current status of application 08/964,388 is not listed. It should be included that the application is now U.S. Patent 6,092,194. Correction is required.

Double Patenting

4. 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. See *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).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321© may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

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).

5. Claims 1,11,21, and 22 are rejected under the judicially created doctrine of double patenting over claims 1,17,18,32,40, and 41 of U. S. Patent No. 6,092,194 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows: It is disclosed of comprising obtaining a downloadable, fetching the downloadable includes one or more references to a component, at least one component identified by the one or more references, and performing a function on the downloadable and all components fetched to generate a downloadable ID. The language "comprising" is open-ended language which contains atleast the listed elements which all the current elements in claims 1,11,21, and 22 of the instant application are taught in claims 1,17,18,32,40, and 41 of U.S. Patent 6,092,194.

Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of the application which matured into a patent.

Claim Rejections - 35 USC § 112

6. 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.

7. Claims 3 and 13 contain the trademark/trade name "ActiveX". Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe an executable type of code and, accordingly, the identification/description is indefinite.

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:

> 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), but 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 only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1,7,8,10,11,17,18,20,21, and 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Apperson et al.

As per claims 1,11,21, and 22, Apperson et al discloses of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege categories that the executable code (downloadable) may try to perform on the client machine (one or more references to a component). The distributing authority digitally signs (performs a function) the executable code and the privilege request code and provides a certificate (generated downloadable ID) that can be traced by a client to a known certifying authority (col. 2, lines 43-53).

As per claims 7 and 17, Apperson et al discloses of performing the function of a SHA-hash (function) on the executable code (col. 4, lines 44-48).

As per claims 8,10,18, and 20, it is taught by Apperson et al of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege

categories (first and all components referenced) that the executable code (downloadable) may try to perform on the client machine (col. 2, lines 43-47).

Claim Rejections - 35 USC § 103

10. 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 negatived by the manner in which the invention was made.

11. Claims 2-4 and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Apperson et al in view of Khare.

It is disclosed by Apperson et al of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege categories that the executable code (downloadable) may try to perform on the client machine (one or more references to a component). The distributing authority digitally signs (performs a function) the executable code and the privilege request code and provides a certificate (generated downloadable ID) that can be traced by a client to a known certifying authority (col. 2, lines 43-53). The teachings of Apperson et al disclose of digitally signing executable code (downloadables), but do not identify that the executable code (downloadable) contains specific privilege request code such as being an applet, ActiveX control, or a plug-in. It is disclosed by Khare of an identical teaching which discloses Microsoft announcing a tool that allows vendors to digitally sign ActiveX

(controls), Java (applets), and plug-in components (pg 1). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply code signing to information such as ActiveX controls, Java applets, and plug-in components. The teachings of Khare disclose that the intent of code signing is to identify a creator of an Internet based applet before a user downloads it and it is designed to provide users with the same level of security found in marketed software which is based on a level of trust and place pressure on independent service vendors (ISVs) honest and the additionally issue digital certificates to the executables (downloadable) components such as ActiveX controls (pg 1). Apperson et al additional recites of motivation that enables servers to download executables (downloadables) with full client validation of their origin and authenticity (col. 2, lines 34-38) and the teachings of Khare are an obvious extension of the teachings of Apperson et al as a means of identifying specific components such as an applet, ActiveX control, or a plug-in to provide a user/client with information about the executable (downloadable) and if it is trusted from an external source and if it has been authenticated.

12. Claims 5,6,9,15,16, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Apperson et al.

As per claims 5,6,15, and 16, it is disclosed by Apperson et al of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege categories that the executable code (downloadable) may try to perform on the client machine (one or more references to a component). The distributing authority digitally signs

(performs a function) the executable code and the privilege request code and provides a certificate (generated downloadable ID) that can be traced by a client to a known certifying authority (col. 2, lines 43-53). The teachings of Apperson et al disclose of digitally signing executable code (downloadables), but do not identify that the executable code (downloadable) contains specific privilege request code such as including HTML code or an application program. The examiner hereby takes official notice that it is notoriously well known that HTML code and application programs include executable code. It would have been obvious to a person of ordinary skill in the art to have been motivated to interpret the teachings of Apperson et al to have included the use of HTML code and application programs as specific forms of executable code. It is notoriously well known that HTML code and application programs are information that is transferred across the Internet and downloaded by a client computer's browser which reads and executes the executable code. An application program is known as being a program in assisting in the performance of a specific task, namely a web based document processing and HTML is known as a markup language used for documents on the World Wide Web and indicates how web browsers should display the elements of a web document to a user. It is obvious that the teachings of Apperson et al could have included HTML code and application code as forms of executable code (downloadables) since it is executable information which is transferred across the Internet.

As per claims 9 and 19, it is taught by Apperson et al of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege categories (first and all components referenced) that the executable code (downloadable) may try

to perform on the client machine (one or more references to a component)(col. 2, lines 43-47). The teachings of Apperson et al are silent in disclosing that the executable code (downloadable) does not include any references. The examiner hereby asserts that it is obvious for the teachings of Apperson et al to make use of this feature. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to include or exclude components in executable code (downloadable). The governing factor would be the intent of the executable code (downloadable) and how it was designed. If it were a independent of any other function within an interactive environment, such as documents on the World Wide Web, then it could be executed independent of any other components once downloaded onto a user's computer. Otherwise, if downloaded executable code was dependent on functions on a user's computer as is explicitly disclosed by Apperson et al (col. 2, lines 43-47), then the specific functions would be referenced by the executable code (downloadable). It is obvious that the teachings of Apperson et al could have include executable code (downloadable) without including any references since there exists various types of executable code that may or may not reference other components.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Touboul et al, U.S. Patent 6,154,844

Touboul, U.S. Patent 6,092,194

"Microsoft ActiveX Software Development Kit"

"Release Notes for the Microsoft ActiveX Development Kit"

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher Revak whose telephone number is (703) 305-1843. The examiner can normally be reached on Monday-Thursday from 6:30 am to 4:00 pm. The examiner can also be reached on alternate Fridays from 6:30 am to 3:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned as follows:

for After-Final Communications:	(703) 746-7238;
for Official Communications:	(703) 746-7239;
for Non-Official Communications:	(703) 746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

CR

June 26, 2003

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Please type a plus sign (+) inside this box +

PTO/SB/08A (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

+ #2

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Group Art Unit	2785
Examiner Name	Unknown
Attorney Docket Number	43426.00011

OIPE
SEP 27 2001
PATENT & TRADEMARK OFFICE

RECEIVED
OCT 01 2001
Technology Center 2100

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		5,077,677		John H. Murphy, et al.	12-31-1991	
		5,359,659		Doren Rosenthal	10-25-1994	
		5,361,359		Homayoon Tajalli, et al.	11-01-1994	
		5,485,409		Sarban Gupta, et al.	01-16-1996	
		5,485,575		David M. Chess, et al.	01-16-1996	
		5,572,643		David H. Judson	11-05-1996	
		5,606,668		Gil Shwed	02-25-1997	
		5,623,600		Shuang Ji, et al.	04-22-1997	
		5,638,446		Aviel D. Rubin	06-10-1997	
		5,692,047		Charles E. McManis	11-25-1997	
		5,692,124		James M. Holden, et al.	11-25-1997	
		5,720,033		Umesh Deo	02-17-1998	
		5,724,425		Sheue-Ling Chang, et al.	03-03-1998	
		5,740,248		Helmut Fieres, et al.	04-14-1998	
		5,761,421		Arthur A. van Hoff, et al.	06-02-1998	
		5,765,205		Franklin Charles Breslau, et al.	06-09-1998	
		5,784,459		Murthy Devarakonda, et al.	07-21-1998	
		5,796,952		Owen Davis, et al.	08-18-1998	
		5,805,829		Geoffrey Alexander Cohen, et al.	09-08-1998	
		5,832,208		Chia-Hwang Chen, et al.	11-03-1998	
		5,850,559		Michael F. Angelo, et al.	12-15-1998	
		5,859,966		Kenneth John Hayman, et al.	01-12-1999	
		5,864,683		William E. Boebert, et al.	01-26-1999	
		5,892,904		Robert G. Atkinson, et al.	04-06-1999	
		5,951,698		Eva Y. Chen, et al.	09-14-1999	
		5,956,481		James E. Walsh, et al.	09-21-1999	
		5,974,549		Gilad Golan	10-26-1999	
		5,983,348		Shuang Ji	11-09-1999	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Office[3]	Number[4]	Kind Code[5] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	6/25/03

*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.

[1] Unique citation designation number. [2] See attached Kinds of U.S. Patent Documents. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark hee if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box → +

PTO/SB/08A (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Group Art Unit	2785
Examiner Name	Unknown
Attorney Docket Number	43426.00011

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials *	Cite No.[1]	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, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		JIM K. OMURA, "Novel Applications of Cryptography in Digital Communications", IEEE Communications Magazine, May, 1990; pages 21-29.	
		OKAMOTO, E. et al., "ID-Based Authentication System For Computer Virus Detection", IEEE/IEE Electronic Library online, Electronics Letters, Vol. 26, Issue 15, ISSN 0013-5194, July 19, 1990, Abstract and pages 1169-1170. URL: http://iel.ihs.com:80/cgi-bin/iel_cgi?se...2ehts%26ViewTemplate%3ddocview%5fb%2ehts.	
		IBM AntiVirus User's Guide Version 2.4, International Business Machines Corporation, November 15, 1995, page 6-7.	
		NORVIN LEACH et al, "IE 3.0 Applets Will Earn Certification", PC Week, Vol. 13, No. 29, July 22, 1996, 2 pages.	
		"Finjan Software Releases SurfinBoard, Industry's First JAVA Security Product For the World Wide Web", Article published on the Internet by Finjan Software Ltd., July 29, 1996, 1 page.	
		"Powerful PC Security for the New World of Java™ and Downloadables, Surfin Shield™" Article published on the Internet by Finjan Software Ltd., 1996, 2 Pages.	
		Microsoft® Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet", Microsoft Corporation, October 1996, including Abstract, Contents, Introduction and pages 1-10.	
		"Finjan Announces a Personal Java™ Firewall For Web Browsers - the SurfinShield™ 1.6 (formerly known as SurfinBoard)", Press Release of Finjan Releases SurfinShield 1.6, October 21, 1996, 2 pages.	
		Company Profile "Finjan - Safe Surfing, The Java Security Solutions Provider" Article published on the Internet by Finjan Software Ltd., October 31, 1996, 3 pages.	
		"Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0" Las Vegas Convention Center/Pavilion 5 P5551, November 18, 1996, 3 pages.	
		"Java Security: Issues & Solutions" Article published on the Internet by Finjan Software Ltd., 1996, 8 pages.	
		"Products" Article published on the Internet, 7 pages.	
		MARK LaDUE, "Online Business Consultant: Java Security: Whose Business Is It?" Article published on the Internet, Home Page Press, Inc. 1996, 4 pages.	
		Web Page Article "Frequently Asked Questions About Authenticode", Microsoft Corporation, last updated February 17, 1997, Printed December 23, 1998. URL: http://www.microsoft.com/workshop/security/authcode/signfaq.asp#9, pages 1-13.	
		ZHANG, X.N., "Secure Code Distribution", IEEE/IEE Electronic Library online, Computer, Vol. 30, Issue 6, June, 1997, Pages: 76-79.	

Examiner Signature		Date Considered	6/25/05

*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.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

OIPE JC44 SEP 21 2001 PATENT & TRADEMARK OFFICE

Notice of References Cited	Application/Control No. 09/539,667	Applicant(s)/Patent Under Reexamination TOUBOUL, SHLOMO	
	Examiner Christopher A. Revak	Art Unit 2131	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,154,844 A	11-2000	Touboul et al.	713/201
	B	US-6,092,194 A	07-2000	Touboul, Shlomo	713/200
	C	US-5,978,484 A	11-1999	Apperson et al.	705/54
	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

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Khare, "Microsoft Authenticode Analyzed" July 22, 1996, xent.com/FoRK-archive/summer96/0338.html, pg 1-2
	V	"Release Notes for the Microsoft ActiveX Development Kit", August 13, 1996, activex.adsp.or.jp/inetsdk/readme.txt, pg 1-10
	W	"Microsoft ActiveX Software Development Kit" August 12, 1996, activex.adsp.or.jp/inetsdk/help/overview.htm, pg 1-6
	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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/539,667	03/30/2000	Shlomo Touboul	~~40492.00011~~ 4242.6	8436

30256 7590 07/01/2003

SQUIRE, SANDERS & DEMPSEY L.L.P
600 HANSEN WAY
PALO ALTO, CA 94304-1043

EXAMINER	
REVAK, CHRISTOPHER A	

ART UNIT	PAPER NUMBER
2131	5

DATE MAILED: 07/01/2003

Response Due: 10/1/2003
FINAL: 1/1/2004

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

DATES ENTERED
Response Due 10/1/2003

JUL 07 2003

CALENDARED
BY
ATTORNEY
SQUIRE, SANDERS & DEMPSEY

PTO-90C (Rev. 07-01)

Office Action Summary	Application No.	Applicant(s)	
	09/539,667	TOUBOUL, SHLOMO	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- 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) 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 the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- 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 _____.

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) 1-22 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) 1-22 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 _____ 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).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ 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.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

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-1449) Paper No(s) 2.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement submitted is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

2. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally ***limited to a single paragraph*** on a separate sheet within the range of 50 to 250 words. It is important that the abstract not exceed 250 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

It is noted by the examiner that the abstract should be amended to be incorporated into a single paragraph.

3. The specification is objected to because the current status of application 08/964,388 is not listed. It should be included that the application is now U.S. Patent 6,092,194. Correction is required.

SOPHOS
EXHIBIT 1004 - PAGE 0584

Double Patenting

4. 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. See *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).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321© may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

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).

5. Claims 1,11,21, and 22 are rejected under the judicially created doctrine of double patenting over claims 1,17,18,32,40, and 41 of U. S. Patent No. 6,092,194 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows: It is disclosed of comprising obtaining a downloadable, fetching the downloadable includes one or more references to a component, at least one component identified by the one or more references, and performing a function on the downloadable and all components fetched to generate a downloadable ID. The language "comprising" is open-ended language which contains atleast the listed elements which all the current elements in claims 1,11,21, and 22 of the instant application are taught in claims 1,17,18,32,40, and 41 of U.S. Patent 6,092,194.

Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of the application which matured into a patent.

Claim Rejections - 35 USC § 112

6. 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.

7. Claims 3 and 13 contain the trademark/trade name "ActiveX". Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe an executable type of code and, accordingly, the identification/description is indefinite.

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:

> 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), but 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 only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1,7,8,10,11,17,18,20,21, and 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Apperson et al.

As per claims 1,11,21, and 22, Apperson et al discloses of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege categories that the executable code (downloadable) may try to perform on the client machine (one or more references to a component). The distributing authority digitally signs (performs a function) the executable code and the privilege request code and provides a certificate (generated downloadable ID) that can be traced by a client to a known certifying authority (col. 2, lines 43-53).

As per claims 7 and 17, Apperson et al discloses of performing the function of a SHA-hash (function) on the executable code (col. 4, lines 44-48).

As per claims 8,10,18, and 20, it is taught by Apperson et al of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege

categories (first and all components referenced) that the executable code (downloadable) may try to perform on the client machine (col. 2, lines 43-47).

Claim Rejections - 35 USC § 103

10. 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 negatived by the manner in which the invention was made.

11. Claims 2-4 and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Apperson et al in view of Khare.

It is disclosed by Apperson et al of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege categories that the executable code (downloadable) may try to perform on the client machine (one or more references to a component). The distributing authority digitally signs (performs a function) the executable code and the privilege request code and provides a certificate (generated downloadable ID) that can be traced by a client to a known certifying authority (col. 2, lines 43-53). The teachings of Apperson et al disclose of digitally signing executable code (downloadables), but do not identify that the executable code (downloadable) contains specific privilege request code such as being an applet, ActiveX control, or a plug-in. It is disclosed by Khare of an identical teaching which discloses Microsoft announcing a tool that allows vendors to digitally sign ActiveX

(controls), Java (applets), and plug-in components (pg 1). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply code signing to information such as ActiveX controls, Java applets, and plug-in components. The teachings of Khare disclose that the intent of code signing is to identify a creator of an Internet based applet before a user downloads it and it is designed to provide users with the same level of security found in marketed software which is based on a level of trust and place pressure on independent service vendors (ISVs) honest and the additionally issue digital certificates to the executables (downloadable) components such as ActiveX controls (pg 1). Apperson et al additional recites of motivation that enables servers to download executables (downloadables) with full client validation of their origin and authenticity (col. 2, lines 34-38) and the teachings of Khare are an obvious extension of the teachings of Apperson et al as a means of identifying specific components such as an applet, ActiveX control, or a plug-in to provide a user/client with information about the executable (downloadable) and if it is trusted from an external source and if it has been authenticated.

12. Claims 5,6,9,15,16, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Apperson et al.

As per claims 5,6,15, and 16, it is disclosed by Apperson et al of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege categories that the executable code (downloadable) may try to perform on the client machine (one or more references to a component). The distributing authority digitally signs

(performs a function) the executable code and the privilege request code and provides a certificate (generated downloadable ID) that can be traced by a client to a known certifying authority (col. 2, lines 43-53). The teachings of Apperson et al disclose of digitally signing executable code (downloadables), but do not identify that the executable code (downloadable) contains specific privilege request code such as including HTML code or an application program. The examiner hereby takes official notice that it is notoriously well known that HTML code and application programs include executable code. It would have been obvious to a person of ordinary skill in the art to have been motivated to interpret the teachings of Apperson et al to have included the use of HTML code and application programs as specific forms of executable code. It is notoriously well known that HTML code and application programs are information that is transferred across the Internet and downloaded by a client computer's browser which reads and executes the executable code. An application program is known as being a program in assisting in the performance of a specific task, namely a web based document processing and HTML is known as a markup language used for documents on the World Wide Web and indicates how web browsers should display the elements of a web document to a user. It is obvious that the teachings of Apperson et al could have included HTML code and application code as forms of executable code (downloadables) since it is executable information which is transferred across the Internet.

As per claims 9 and 19, it is taught by Apperson et al of providing executable code (downloadable) with privilege request code that indicates (fetches) a set of privileges or privilege categories (first and all components referenced) that the executable code (downloadable) may try

to perform on the client machine (one or more references to a component)(col. 2, lines 43-47). The teachings of Apperson et al are silent in disclosing that the executable code (downloadable) does not include any references. The examiner hereby asserts that it is obvious for the teachings of Apperson et al to make use of this feature. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to include or exclude components in executable code (downloadable). The governing factor would be the intent of the executable code (downloadable) and how it was designed. If it were a independent of any other function within an interactive environment, such as documents on the World Wide Web, then it could be executed independent of any other components once downloaded onto a user's computer. Otherwise, if downloaded executable code was dependent on functions on a user's computer as is explicitly disclosed by Apperson et al (col. 2, lines 43-47), then the specific functions would be referenced by the executable code (downloadable). It is obvious that the teachings of Apperson et al could have include executable code (downloadable) without including any references since there exists various types of executable code that may or may not reference other components.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Touboul et al, U.S. Patent 6,154,844

Touboul, U.S. Patent 6,092,194

"Microsoft ActiveX Software Development Kit"

"Release Notes for the Microsoft ActiveX Development Kit"

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher Revak whose telephone number is (703) 305-1843. The examiner can normally be reached on Monday-Thursday from 6:30 am to 4:00 pm. The examiner can also be reached on alternate Fridays from 6:30 am to 3:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned as follows:

for After-Final Communications:	(703) 746-7238;
for Official Communications:	(703) 746-7239;
for Non-Official Communications:	(703) 746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

CR

June 26, 2003

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

US005978484A

United States Patent [19]

Apperson et al.

[11] Patent Number: 5,978,484

[45] Date of Patent: Nov. 2, 1999

[54] **SYSTEM AND METHOD FOR SAFETY DISTRIBUTING EXECUTABLE OBJECTS**

[75] Inventors: **Norman Apperson**, Bellevue; **Brian C. Beckman**, Renton, both of Wash.

[73] Assignee: **Microsoft Corporation**, Redmond, Wash.

[21] Appl. No.: **08/639,290**

[22] Filed: **Apr. 25, 1996**

[51] **Int. Cl.**[6] **H04K 1/00**; H04L 9/00

[52] **U.S. Cl.** **380/25**; 380/4

[58] **Field of Search** 380/25, 24, 23, 380/4; 395/157

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,868,877	9/1989	Fischer	380/25
5,005,200	4/1991	Fischer	380/25
5,214,702	5/1993	Fischer	380/25
5,311,591	5/1994	Fischer	380/4
5,412,717	5/1995	Fischer	380/25
5,412,774	5/1995	Agrawal	395/157
5,692,047	11/1997	McManis	380/4
5,745,574	4/1998	Muftic	380/25
5,825,877	10/1998	Dan et al.	380/25

OTHER PUBLICATIONS

Schneier, Bruce, "Applied Cryptography, Second Edition: Protocols, Algorigthms, and Source Code in C," (1996), pp. 574–577.

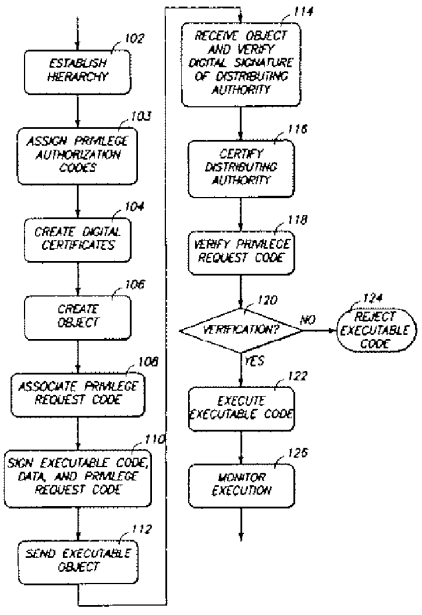
Bank, Joseph A., "Java Security," (Dec. 8, 1995), found at Internet URL http://swissnet.ai.mit.edu/~jbank/javapaper/javapaper.html/.

Primary Examiner—Benjamin R. Fuller
Assistant Examiner—Robin Clark
Attorney, Agent, or Firm—Lee & Hayes, PLLC

[57] **ABSTRACT**

The invention includes a method and system for distributing and executing executable code. Before sending executable code to a client, a distributing authority associates a privilege request code with the executable code. The privilege request code indicates a requested set of privileges that the executable code will potentially exercise during execution. The distributing authority digitally signs the executable code and associated privilege request code and then distributes it for eventual execution by clients. Before executing the executable code, a client verifies the digital signature to confirm the authenticity and integrity of the executable code and associated privilege request code. This verification utilizes a hierarchy of certifying authorities. While the code executes, the client monitors it and prevents it from exercising privileges that are not in the requested set of privileges.

20 Claims, 4 Drawing Sheets



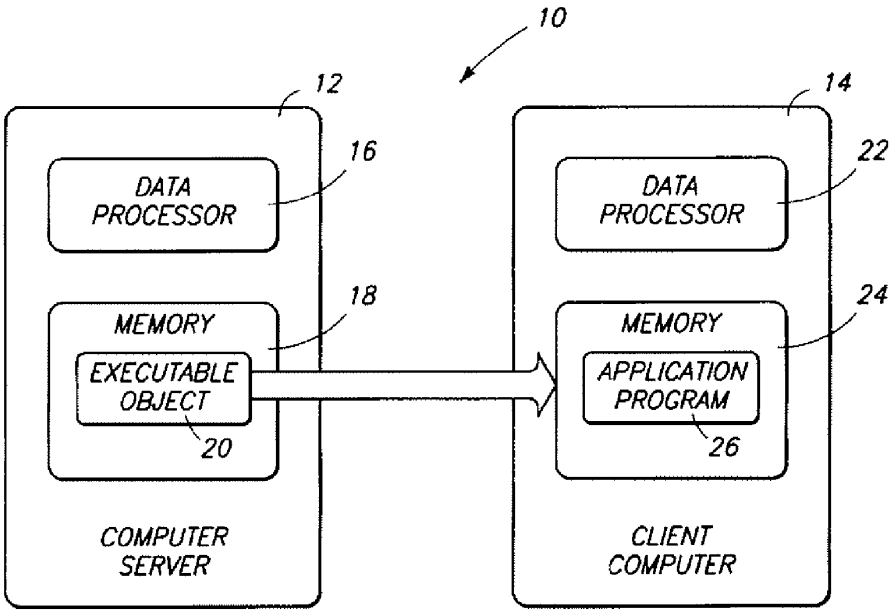

10
12
14
16
22
DATA PROCESSOR
DATA PROCESSOR
18
24
MEMORY
MEMORY
EXECUTABLE OBJECT
20
APPLICATION PROGRAM
26
COMPUTER SERVER
CLIENT COMPUTER

Fig 1

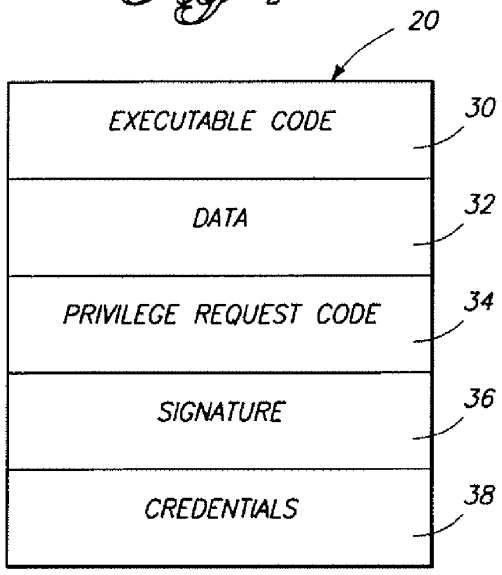

20
EXECUTABLE CODE
30
DATA
32
PRIVILEGE REQUEST CODE
34
SIGNATURE
36
CREDENTIALS
38

Fig 2

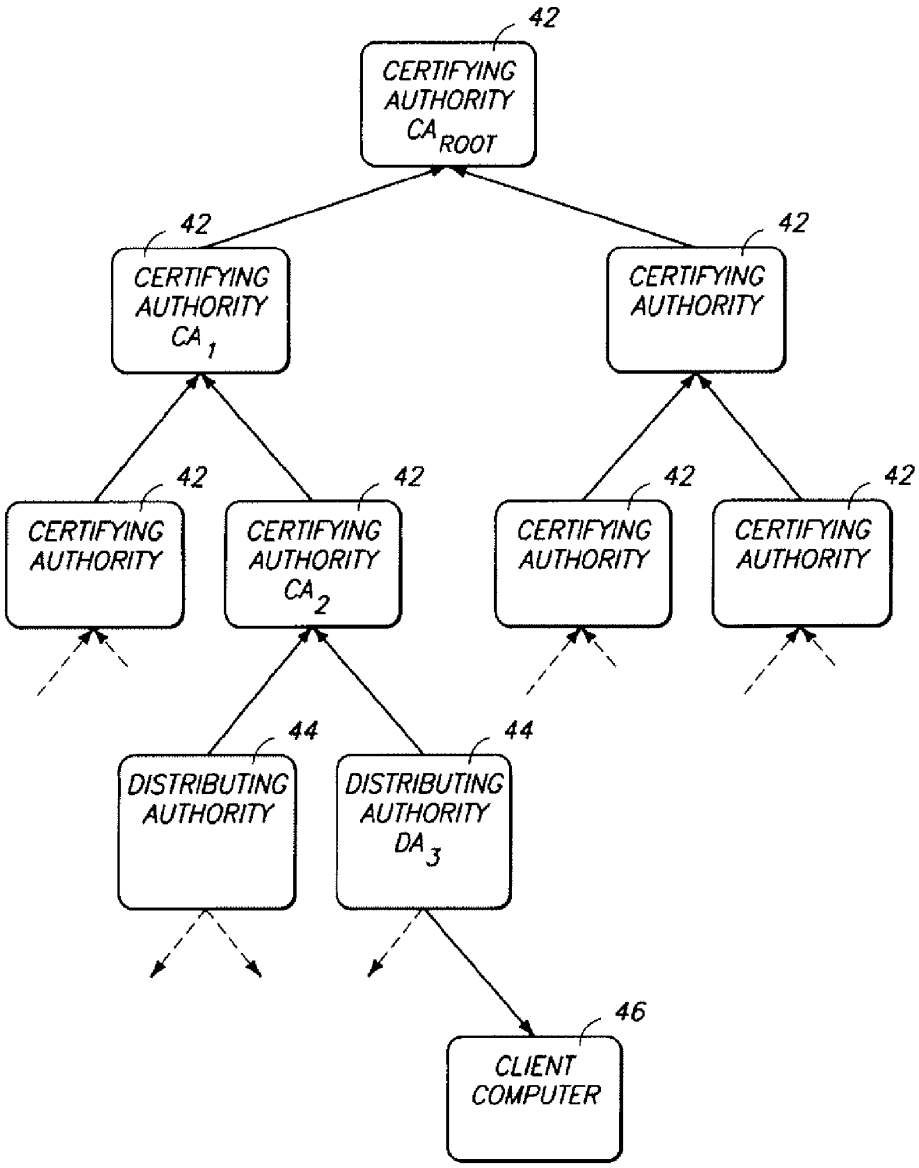

42
CERTIFYING AUTHORITY CA ROOT
42
CERTIFYING AUTHORITY CA 1
42
CERTIFYING AUTHORITY
42
CERTIFYING AUTHORITY
42
CERTIFYING AUTHORITY CA 2
42
CERTIFYING AUTHORITY
42
CERTIFYING AUTHORITY
44
DISTRIBUTING AUTHORITY
44
DISTRIBUTING AUTHORITY DA 3
46
CLIENT COMPUTER

Fig 3

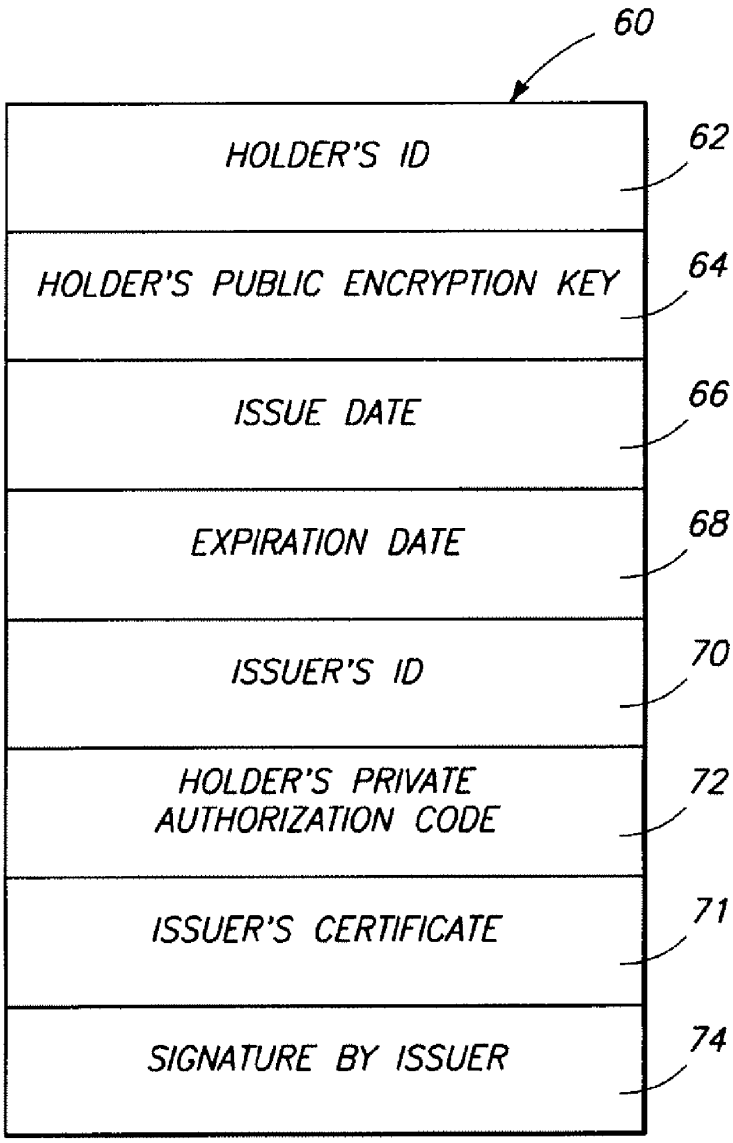

60
HOLDER'S ID
62
HOLDER'S PUBLIC ENCRYPTION KEY
64
ISSUE DATE
66
EXPIRATION DATE
68
ISSUER'S ID
70
HOLDER'S PRIVATE AUTHORIZATION CODE
72
ISSUER'S CERTIFICATE
71
SIGNATURE BY ISSUER
74

Fig 4

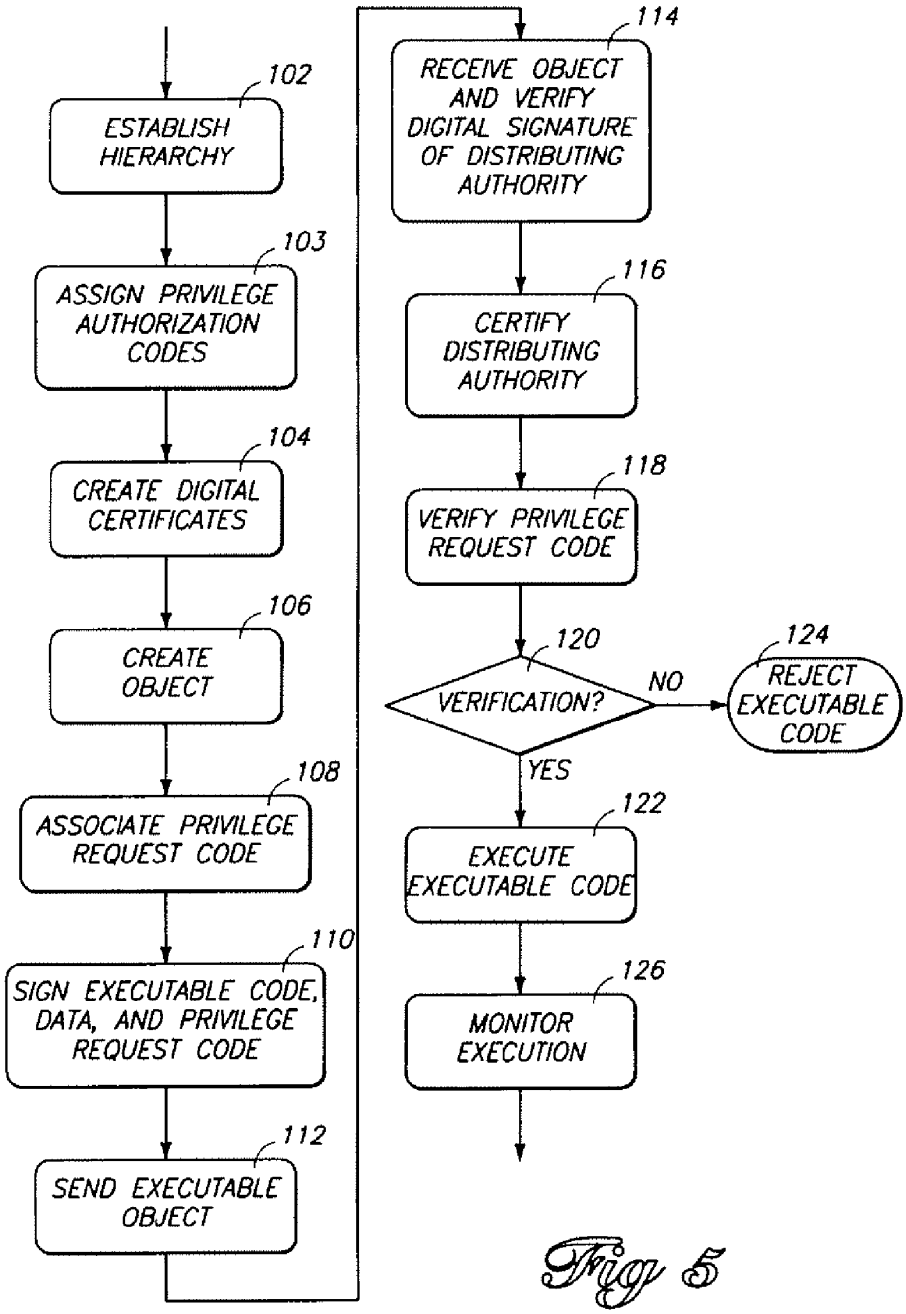

102
ESTABLISH HIERARCHY
103
ASSIGN PRIVILEGE AUTHORIZATION CODES
104
CREATE DIGITAL CERTIFICATES
106
CREATE OBJECT
108
ASSOCIATE PRIVILEGE REQUEST CODE
110
SIGN EXECUTABLE CODE, DATA, AND PRIVILEGE REQUEST CODE
112
SEND EXECUTABLE OBJECT
114
RECEIVE OBJECT AND VERIFY DIGITAL SIGNATURE OF DISTRIBUTING AUTHORITY
116
CERTIFY DISTRIBUTING AUTHORITY
118
VERIFY PRIVILEGE REQUEST CODE
120
VERIFICATION?
NO
124
REJECT EXECUTABLE CODE
YES
122
EXECUTE EXECUTABLE CODE
126
MONITOR EXECUTION

Fig 5

SYSTEM AND METHOD FOR SAFETY DISTRIBUTING EXECUTABLE OBJECTS

TECHNICAL FIELD

This invention relates to client-server environments in which executable objects are downloaded or otherwise distributed from a distributing authority and executed on a different computer.

BACKGROUND OF THE INVENTION

There has been a dramatic increase in reliance upon service providers accessible via electronic data communications networks such as the Internet. Such service providers are generally interested in providing access to the widest possible client audience at the lowest cost. Very recently, a number of solutions have emerged that allow service providers to achieve these goals. In particular, there has been very rapid growth in the use of the standardized hypertext capabilities of the World Wide Web (WWW) on the Internet. The standardized nature of the WWW, as well as the very low costs involved in accessing the Internet, have eliminated many of the previous hurdles to service development and distribution.

While the Internet's World Wide Web and other similar environments allow service providers to build systems that can efficiently deliver information to potentially large numbers of clients, they also impose limitations. These limitations are a direct consequence of the desire to provide a simple, generic processing model for multiple purposes.

It has been recognized that these limitations can be addressed to some degree by allowing servers to send executable code to clients, for execution by the clients themselves. This allows a server to build client software for a specific purpose, thereby allowing the service provider to add functionality to existing client software. An advantage of this approach is that it can in many cases reduce both the processing burdens on the server and the communications requirements between the server and the client.

While it might be very desirable for a client to execute server-provided software, the potential threat to security is a serious drawback. For a client to be willing to execute server-defined functionality, the client must be assured that no adverse effects will occur. Specifically, there must be a guarantee that existing client data will not be read or modified and that hostile code (viruses, Trojan horses, etc.) will not be generated and installed on the client system.

This is particularly problematic in the public network environment since mechanisms for establishing trust between a client and server are not widely deployed, and data communications channels are open to eavesdropping and tampering. Because of this, general purpose compiled programming languages are not a solution. It is inherently unsafe in a public network environment for a client to accept binary executable images from a server and execute them. Since the server-provided programs would have access to the full resources of the client computer environment, they could potentially perform any of various different types of dangerous or hostile operations.

Binary executable code also has the disadvantage of being architecture-specific. It is a significant complication for the server to determine the computer hardware in use by the client and the operating system, and to provide different executable modules for use with different systems.

These issues lead naturally to consideration of an interpreted language. This approach allows a server to create

program scripts that can be executed on the client to extend its functionality, while providing a more controlled execution environment and architecture neutrality. Interpreters can be implemented on a variety of computer platforms and operating systems to provide an isolation layer between the language specification and the underlying architecture. Hence, a server can provide scripts for extensions that are executable on a variety of client machines. Interpreters can also perform runtime checking of various sorts to enforce access of specific resources and to detect when scripts have been tampered with. Sun Microsystem's recently announced Java language is an example of this approach.

From a client's perspective, the optimal situation is one in which it needs only trust the interpreter. Once a client has an interpreter from a trusted source, the client should be able to execute any script with complete safety. This is where existing approaches fail. Java, for example, is a general purpose programming environment which allows the generation of complex applications including I/O operations. Java is specifically designed to allow easy access to network facilities, hence it has the potential to surreptitiously transmit client confidential information; destroy client data, and perform other hostile actions. The protection against such behavior relies on the ability to validate Java scripts and determine their authenticity. Importantly, however, Java and many other systems rely on a trust relationship between the server and the client as the basis for their safety. We believe that this is a significant limitation which our invention addresses.

In addition to eliminating the requirement of a trust relationship between the client and server, our invention provides for situations in which a client may wish to execute server-provided code that performs I/O and other potentially dangerous operations. Our invention provides a secure extension mechanism that enables servers to download general purpose executables with full client validation of their origin and authenticity.

SUMMARY OF THE INVENTION

The invention classifies different types of security-related operations and services, which might potentially be performed by externally-provided code, into different categories. When providing executable code, a distributing authority also provides a privilege request code, indicating a set of privileges or privilege categories that the executable code might perform on the client machine. The distributing authority digitally signs the executable code and the privilege request code, and also provides a certificate that can be traced by the client to a known certifying authority. The certificate indicates an authorized set of privileges that the distributing authority has been authorized to include in distributed code.

The certificate is issued to the distributing authority by a certifying authority that is a member of a hierarchy of authorities. The certificate is signed by the certifying authority, and includes or refers to the certificate of an even higher certifying authority. Each certificate therefore relies for its verification upon a higher certifying authority, except for a root authority that is known to be trustworthy.

Each certificate indicates an authorized set of privileges that the holder of the certificate is authorized pass on to lower members of the hierarchy. When a distributing authority distributes actual executable code, the associated privilege request code must indicate a subset of the privileges indicated by the privilege authorization code of the certificate held by the distributing authority. Before executing

FJN 013119
SOPHOS
EXHIBIT 1004 - PAGE 0598

code provided from some external source such as a server, the client traces the authority of the distributing authority that signed the code, through one or more certifying authorities to one that is known to the client independently of the server. For each certifying authority, the client verifies that the privilege authorization code indicates privileges that are a subset of the privileges indicated by the certificate of the next-higher certifying authority.

If the client verifies the signature and digital certificate of the distributing authority by tracing to an authority that is already known to the client, the client executes the provided code. However, it monitors the code, and prevents it from exercising any privileges that are not indicated in the associated privilege request code.

In practice, the client creates a granted privilege set for a particular executable object, and prevents the object from exercising any privileges not in the granted privilege set. The granted privilege set is preferably created by intersecting the privilege authorization sets from the digital certificate of the distributing authority and of any higher authorities encountered while tracing the certificate of the distributing authority. Any failure while checking the authority of the distributing authority results in an empty granted privilege set. Every executable statement in the executable object is then checked against the granted privilege set before execution.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a computer system in accordance with the invention.

FIG. **2** is a block diagram of an executable object in accordance with the invention.

FIG. **3** is a block diagram of a hierarchy of authorities in accordance with the invention.

FIG. **4** is illustrates an example of a digital certificate in accordance with the invention.

FIG. **5** is a flow chart showing preferred methodical steps in accordance with the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The invention described below utilizes well-known digital encryption and signing techniques. The following discussion therefore assumes familiarity with these topics. For example, the invention utilizes public-key cryptography techniques such as described in Schneier, Bruce; *Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C*; New York: John Wiley & Sons, 1996, which is hereby incorporated by reference. Particularly, the invention utilizes the RSA (Rivest, Shamir, and Adlemen) public-key algorithm for digital signatures, in conjunction with a hashing algorithm referred to as SHA (secure hash algorithm), although other public-key signature schemes, such as DSS, ElGamal, Elliptic Curve, can alternatively be used.

FIG. I shows a computer system **10** in accordance with a preferred embodiment of the invention. Computer system **10** includes a computer server **12** and a client computer **14**. Computer server **12** includes a data processor **16**, a computer-readable storage medium or memory **18**, and other components (not shown) typical of a computer network server. Memory **18** includes both electronic and magnetic or optical mass storage memory.

Computer server **12**, in this case also referred to as a distributing authority, is configured to provide or distribute one or more signed executable objects **20** for execution by client computer **14**. An object **20** is initially stored by server **12** in memory **18**. Computer server **12** is connected to download such executable objects to client computer **14** over a communications channel or link, such as a local area network connection, a wide area network connection, or a remote connection from an online service provider. The executable objects comprise both executable code and associated data. The code might be in the form of textual scripts, byte codes, P-code, or binary object code.

Client computer **14** is similarly connected to download and execute executable objects **20** from the computer server. Client computer **14** includes a processing unit or data processor **22** and memory **24**. Memory **24** includes electronic and optional mass-storage memory such as a magnetic or optical storage medium. Client computer **14** includes other components (not shown) such as are commonly incorporated in a personal or desktop computer.

An application program **26** executes on data processor **22** from memory **24**. The application program in the preferred embodiment of the invention is a client program that interacts with computer server **20**. As an example, application program **26** might be a "browser" application such as is commonly used to access resources on a public network such as the Internet or on a private "intranet." The client program is configured to accept and execute executable code provided by computer server **20**.

FIG. **2** shows preferred components of executable object **20**. The object includes executable code **30**, associated data **32**, a privilege request code **34**, a digital signature **36**, and digital credentials **38**.

Privilege request code **34** is a code that indicates a set of security-related privileges that executable code **30** of object **20** will potentially execute on client **14**. The facilities of the client operating system or script interpreter are divided up into a set of privileges or privilege classes. In the Windows NT® operating system for example, these privilege classes might relate individually to file I/O, network operations, registry read/write rights, graphics operations, window management, and user list read/write rights. The privilege request code indicates which of these classes of services are potentially required by executable code **30**.

Digital signature **36** is a digital signature of the concatenated executable code, data, and privilege request code from the executable object **20**. More particularly, this is an RSA-encrypted SHA-hash of the concatenated executable code, data, and privilege request code. This signature can be verified by a client computer to confirm the authenticity and integrity of the executable code, data, and associated privilege authorization code. As will be explained more fully below, the digital signature has the further important property that it can be verified without relying on the trustworthiness of server **12**.

Credentials **38**, associated with the server computer or distributing authority, include a privilege authorization code indicating which privileges or privilege classes are allowed to be exercised by code distributed from server **12** or another distributing authority. The credentials are issued to server **12** or to a distributing authority by one or more certifying authorities and are digitally signed by the certifying authorities. The digital signature of at least one of the certifying authorities can be verified by the client without relying on the trustworthiness of the server or other distributing authority, as will be demonstrated below.

The certifying authorities are responsible for verifying the trustworthiness of the distributing authority that provided

the executable code and the level of trust that should be placed in the executable code and distributing authority. More specifically, the certifying authorities determine which privileges any particular server or distributing authority should be allowed to authorize. For instance, a certifying authority might issue credentials to one distributing authority allowing it to distribute code that exercises a full range of security-related privileges on a client computer, while the executable code from another distributing authority might be precluded from performing file I/O.

Note that in the case shown in FIG. **1**, server **12** is a distributing authority. While this configuration has advantages, executable code might be signed by a distributing authority that is independent of the actual server that provides the code to client **14**. In fact, the distribution path from a distributing authority to a client computer might take many forms. In the example shown, the distribution path is a network connection formed between a server (acting as the distributing authority) and a client of the server. In other cases, the executable code might be distributed by floppy disk or some other portable storage medium from a distributing authority to a user's computer. In still other cases, the executable code might be provided to various online servers from the distributing authorities, and users would obtain the executable code from the servers. In each of these cases, the executable code and associated privilege request code would be signed by the distributing authority, even though the code might be obtained by a user from an entity that has no direct connection to the distributing authority—such as an independent online service provider. In this latter, case, the online service provider would act as a code repository, without participating directly in security measures. Thus, while the service provider might not wish to participate in the security scheme described herein, a client computer could nevertheless rely on the verifiable digital signature of the distributing authority to establish the trustworthiness of the executable code.

The certifying authorities and distributing authorities are members of a hierarchy of authorities as shown in FIG. **3**. The members of the hierarchy have different levels of authority, depending on their positions in the hierarchy and the privileges granted them by higher levels of the hierarchy. The structure of the hierarchy resembles a tree structure, with a "root" member at the top connected to lower "leaf" members by "branches." This "tree of trust" is utilized to verify signatures of distributing authorities and certifying authorities, and to verify the authority of a distributing authority to distribute code with a particular privilege request code.

At the top of the hierarchy is a "root" certifying authority **40**, also designated CA_{ROOT}. This entity has authority over all possible privileges that an executable object might potentially exercise. Beneath the root are different levels of certifying authorities **42**, including a plurality of distributing authorities **44**. Each certifying authority has authority over a potentially different set of privileges.

Each certifying authority and distributing authority is assigned a privilege authorization code by the next-higher certifying authority in the hierarchy. The privilege authorization code of any particular authority indicates a set of privileges that can be authorized by that authority. In addition, the privilege authorization code indicates whether an entity is authorized to certify lower members of the hierarchy and whether the entity is authorized to act as a distributing authority. The privilege authorization code held by any particular entity must indicate a subset of the privileges indicated by the privilege authorization code of the next-higher authority.

In general, any certifying authority can also act as a distributing authority. When acting as a certifying authority, an entity grants or assigns privilege authorization codes to lower members of the hierarchy. The granted privilege authorization codes must indicate a subset of the privileges indicated by the certifying authority's own privilege authorization code. When acting as a distributing authority, an entity distributes executable objects that include privilege request codes. Each such privilege request code must indicate a subset of the privileges indicated by the distributing authority's privilege authorization code.

With this structure, each lower level of authority in the hierarchy potentially has less and less authority for granting privileges to other members of the hierarchy or for distributing executable objects.

In the example of FIG. **3**, a client computer **46** receives an executable object from a distributing authority **44** designated as DA_3. The executable object is signed by DA_3 and includes the privilege authorization code of DA_3. Distributing authority DA_3, in turn, receives its privilege authorization code from a certifying authority CA_2; DA_3's privilege authorization code is a subset of CA_2's privilege authorization code. CA_2 receives its privilege authorization code from a higher certifying authority CA_1, and CA_1 receives its privilege authorization code from the root certifying authority CA_{ROOT}. CA_{ROOT} has a privilege authorization code that includes all possible privileges that might be exercised by executable objects.

To enforce this scheme, the authority of each certifying authority and distributing authority is recorded in a digital certificate, issued and signed by the next higher member of the hierarchy. The credentials discussed above comprise such a digital certificate.

FIG. **4** shows an example of a digital certificate **60**. It includes an identification **62** of the holder of the certificate, the public encryption key **64** of the holder, the date **66** the certificate was issued, the date **68** of its expiration, the privilege authorization code **72** authorized for the holder of the certificate by the certifying authority that issued the certificate, and an identification **70** of the certifying authority that issued the certificate (at the next higher level of the hierarchy). It also includes or refers to the certificate **71** of the certifying authority. Certificate **60** is digitally signed by the certifying authority, using the private signature key of the certifying authority. The digital signature **74** of the certifying authority is appended to and becomes part of the certificate.

The certificate of the root certifying authority is slightly different in that it does not include the certificate or digital signature of any higher authority. Its privilege authorization code indicates all possible privileges.

This scheme results in a chain of digital certificates leading from a distributing authority all the way up the hierarchy to the root certifying authority. The chain of certificates can be traced upward through the hierarchy until reaching the certificate of an authority whose digital signature can be verified without relying on information obtained from the distributing authority.

Referring back to FIG. **3**, assume that distributing authority DA_3 downloads or otherwise provides a signed executable object that is eventually executed by client computer **46**. The object includes credentials of distributing authority DA_3, comprising a digital certificate as described above. The digital certificate includes the public signing key of distributing authority DA_3, allowing client computer **46** to verify the digital signature performed by distributing authority

FJN 013121
SOPHOS
EXHIBIT 1004 - PAGE 0600

DA_3 on the executable code and the privilege request code. The digital certificate also indicates information relating to the certifying authority CA_2 that issued the certificate, including the certificate of certifying authority CA_2.

The certificate of distributing authority DA_3, issued and signed by nexthigher certifying authority CA_2, verifies or confirms the public signing key and the privilege authorization code of distributing authority DA_3. The signature and privilege authority of certifying authority CA_2 can in turn be verified through information in CA_2's digital certificate, issued by certifying authority CA_1.

Now suppose that certifying authority CA_1 is known to the client computer, independently of the executable object. If this is the case, client computer **46** can verify the certificate of certifying authority CA_2 without tracing any farther up the hierarchy. That is, client computer **46** will know the public signing key of certifying authority CA_1, independently of the downloaded executable object, and will thus be able to verify that CA_1 signed the digital certificate of certifying authority CA_2. Client computer **46** can rely on the known trustworthiness of certifying authority CA_1 to confirm the trustworthiness (and digital signature) of CA_2, and can then rely on the trustworthiness of CA_2 to confirm the trustworthiness (and digital signature) of CA_3.

Any certificate (except the certificate of the root authority) can be traced to a higher authority by following the chain of digital certificates up the hierarchy. As used here, the term "tracing" refers to the process of following a chain of digital certificates up through a hierarchy of authorities, while verifying the signature and authority of any particular member of the hierarchy with reference to a certificate that is digitally signed and authorized by a higher level of the hierarchy.

The invention includes a method as illustrated in FIG. **5** of distributing and executing executable objects or code. The method includes a first step **102** of establishing a hierarchy of authorities comprising a plurality of certifying authorities, including the root authority, and a plurality of distributing authorities. The members of the hierarchy are preferably computers connected for communications over a network or other communications medium.

The method includes a step **103** of assigning a privilege authorization code to each member of the hierarchy. The privilege authorization code of any particular member of the hierarchy indicates a set of privileges that the particular member is authorized to incorporate in executable objects that might be provided from that member for execution on other computers. In addition, the privilege authorization code indicates the maximum set of privileges that member can include in the assigned privilege authorization codes of other, lower members of the hierarchy. According to this scheme, the privilege authorization code of any member is assigned to that member by a higher member of the hierarchy, and indicates a subset of the privileges indicated in the privilege authorization code of the higher member.

Step **104** includes creating and signing a digital certificate for each member of the hierarchy, wherein the certificate of any particular member (except that of the root authority) includes or refers to the digital certificate of that higher member. This results in a chain of certificates and corresponding digital signatures, as already described, that can be used for certifying the trustworthiness and authority of any particular member of the hierarchy. The digital certificate of a member also includes the privilege authorization code for that member, assigned to that member by a higher member of the hierarchy.

A step **106**, performed by a distributing authority that is a member of the hierarchy of authorities, comprises creating an executable object as shown in FIG. **2**. The object includes executable code and optional data, as well as signed credentials of the distributing authority. In the preferred embodiment of the invention, the credentials comprise the digital certificate of the distributing authority, formatted as shown in FIG. **4**.

Step **108**, also performed by the distributing authority, comprises associating a privilege request code with the executable code and the optional data. The privilege request code indicates a requested set of privileges that the executable code will potentially exercise on a client computer during execution. The requested set of privileges is a subset of the authorized set of privileges indicated the distributing authority's credentials.

A step **110** comprises digitally signing the executable code, any associated data, and the associated privilege request code. This step is performed by the distributing authority, using its private signing key. Specifically, the distributing authority produces an SHA hash of the concatenated executable code, data, and privilege request code, and encrypts the hash using an RSA encryption algorithm in conjunction with the distributing authority's private signing key.

Step **112** comprises sending or otherwise distributing the executable object, including the privilege request code, credentials and digital signature of the distributing authority, from the distributing authority to a client computer. This step might make use of a network communications medium, or might take place using a portable storage medium such as a floppy disk.

Step **114**, performed by the client computer, comprises receiving the object sent in step **112** and verifying the digital signature of the distributing authority to confirm the authenticity and integrity of the executable code, associated data, and associated privilege request code. This step is performed by decrypting (using the RSA algorithm) the digital signature with the public signing key of the distributing authority (as set forth in the credentials of the distributing authority) and comparing this with an SHA hash of the concatenated executable code, data, and privilege request code.

Step **116**, also performed by the client computer, comprises certifying the trustworthiness of the distributing authority, the validity of the privilege request code, and the authenticity of the distributing authority's credentials. This step includes verifying the digital signature of at least one certifying authority that signed the credentials of the distributing authority, in a way that is not dependent on the trustworthiness of the distributing authority itself. More broadly, this step comprises tracing the chain of digital signatures, contained in the certificate of the distributing authority, to one that can be verified without relying on the trustworthiness of the distributing authority. This involves first verifying the signature of a first member of the hierarchy that signed the credentials or certificate of the distributing authority, then verifying the signature of a second member that signed the certificate of the first member, and so on up the chain of authorities until reaching a digital signature that can be verified without relying on information derived from the certificate of the distributing authority—such as a signature that can be verified using a public signing key that is already known to the client computer.

When tracing the chain of digital signatures, the client computer performs a step of verifying that each particular certificate's indicated authorized set of privileges (indicated

FJN 013122
SOPHOS
EXHIBIT 1004 - PAGE 0601

by its privilege authorization code) is a subset of the authorized set of privileges indicated in the digital certificate of the next-higher member of the hierarchy that digitally signed the particular certificate.

A further step **118** comprises verifying that the privilege request code included in the executable object indicates a set of requested privileges that is a subset of the privileges indicated by the privilege authorization code of the distributing authority. This step is necessary to ensure that the distributing authority has not exceeded its granted authority.

Decision block **120** indicates the action taken as a result of the verification steps performed by the client computer. If these steps indicate that no certifying or distributing authority has exceeded its granted authority, and that all digital signatures are valid, step **122** is performed of executing the executable code. Otherwise, the executable code is rejected, as indicated by termination block **124**.

During execution, as indicated by step **126**, the executable code is monitored to prevent it from exercising unauthorized privileges. Specifically, this involves preventing the executable code from exercising any privileges that are not in the requested set of privileges indicated by the privilege request code. This inherently prevents exercise of any privileges that are not in the authorized set of privileges of the certifying authority that signed the certificate of the distributing authority, as well as any privileges not indicated by the privilege authorization codes of the higher certifying authorities encountered while tracing the chain of digital signatures.

The monitoring step can be implemented by an interpreter, if the executable code is a script, or by use of operating system facilities if the executable code is a binary executable. The Windows NT® operating system, for example, allows strict control over which operations can be performed by individual executing programs. In the future, it might be possible to modify the Windows® operating system to integrate more fully with the scheme described herein.

The methods described above are advantageous because they do not require a trust relationship between a server and its client, or even between the distributing authority and the eventual user of the executable code. Maintaining trust relationships with a plurality of servers or distributing authorities would be troublesome because of the potentially great number of such entities. Using the scheme described above, however, a client can maintain a trust relationship with a fewer number of certifying authorities at higher levels of the hierarchy, and rely on the enforceable safety and security policy maintained by the root authority and other certifying authorities within the hierarchy.

As a further feature, each client can maintain its own database describing the sets of privileges the client is willing to grant different authorities. Each such set is indicated by a signer-specific privilege code, indicating a signer-specific set of privileges. These sets exist independently of any downloaded executable code. Before executing any particular executable object, the client identifies all members whose certificates have been referred to in the credentials of the distributing authority. This includes the certificates of all hierarchy members in the chain of authorities above the distributing authority, all the way up to the root authority. The client then checks its database to see whether any signer-specific privilege codes exist for these members, and takes the intersection of the privileges indicated by any such signer-specific privilege codes. The executable object is prevented from exercising any privileges that are not in this intersection.

In practice, the client creates a granted privilege set for a particular executable object, and prevents the object from exercising any privileges not in the granted privilege set. The granted privilege set is preferably created by intersecting the privilege authorization sets from the digital certificate of the distributing authority and of any higher members encountered while tracing the certificate of the distributing authority. If signer-specific privilege sets exist for any of these hierarchy members, they are intersected with the results of the previous intersection, and the executable object is prevented from executing any privileges not included in the resulting intersection set.

It is advantageous to maintain privilege sets as bit vectors: multi-bit codes wherein each bit corresponds to a specific privilege or classification of privileges. Using this format, intersections can be easily performed by simple logical operations, such as logically ANDing the vectors.

In compliance with the statute, the invention has been described in language more or less specific as to structural and methodical features. It is to be understood, however, that the invention is not limited to the specific features described, since the means herein disclosed comprise preferred forms of putting the invention into effect. The invention is, therefore, claimed in any of its forms or modifications within the proper scope of the appended claims appropriately interpreted in accordance with the doctrine of equivalents.

We claim:

1. A method of distributing and executing executable code, comprising:

creating digital certificates for a plurality of distributing authorities, each such digital certificate indicating an authorized set of privileges for its distributing authority;

associating a privilege request code with the executable code, the privilege request code indicating a requested set of privileges that the executable code will potentially exercise during execution;

defining signer-specific privilege sets at a client computer for different ones of the plurality of distributing authorities, each signer-specific privilege set indicating privileges allowed to executable code signed by the corresponding distributing authority;

digitally signing the executable code and associated privilege request code by a particular one of the plurality of distributing authorities;

receiving the executable code, associated privilege request code, and digital signature at the client computer;

preventing the executable code from executing if the digital signature of the executable code and associated privilege request code cannot be verified;

preventing the executable code from executing if the privilege request code indicates privileges that are not in the signer-specific privilege set of the distributing authority that signed the executable code.

2. A method as recited in claim **1**, further comprising preventing the executable code from exercising privileges that are not indicated by the privilege request code.

3. A method as recited in claim **1**, further comprising:

digitally signing the digital certificate of said particular distributing authority by one or more certifying authorities;

before executing the executable code, verifying the digital signature of at least one of the certifying authorities without relying on the trustworthiness of said particular distributing authority.

4. A method as recited in claim 1, further comprising:

certifying the trustworthiness of said particular distributing authority with a chain of digital signatures by one or more certifying authorities;

associating the chain of digital signatures with the executable code;

before executing the executable code, tracing the chain of digital signatures to one that can be verified without relying on the trustworthiness of said particular distributing authority.

5. A method as recited in claim 1, wherein said particular distributing authority is a memory of a hierarchy of authorities, further comprising the following step:

creating digital certificates for members of the hierarchy, wherein the digital certificate of a particular member is signed by a higher member of the hierarchy and refers to the signed digital certificate of said higher member.

6. A method as recited in claim 1, wherein said particular distributing authority is a memory of a hierarchy of authorities, further comprising the following steps:

creating digital certificates for members of the hierarchy, wherein the digital certificate of a particular member is signed by a higher member of the hierarchy and refers to the signed digital certificate of said higher member;

before executing the executable code, tracing the digital certificate of the distributing authority that signed the executable code to an upper member of the hierarchy of authorities whose digital signature can be verified without relying on the trustworthiness of said particular distributing authority.

7. A method as recited in claim 1, wherein said distributing authority is a memory of a hierarchy of authorities, further comprising the following steps:

creating digital certificates for members of the hierarchy, wherein the digital certificate of a particular member is signed by a higher member of the hierarchy and refers to the signed digital certificate of said higher member;

before executing the executable code, tracing the digital certificate of said particular distributing authority to an upper member of the hierarchy of authorities whose digital signature can be verified without relying on the trustworthiness of said particular distributing authority;

when tracing the digital certificate of said particular distributing authority, verifying that each particular certificate's indicated authorized set of privileges is a subset of the authorized set of privileges indicated in the digital certificate of the higher member that digitally signed the particular digital certificate.

8. A method of distributing and executing executable code, comprising:

creating digital certificates for a plurality of distributing authorities, each such digital certificate indicating an authorized set of privileges for its distributing authority;

defining signer-specific privilege sets at a client computer for different ones of the distributing authorities, each signer-specific privilege set indicating privileges allowed to executable code signed by the corresponding distributing authority;

digitally signing the executable code by one of the plurality of distributing authorities;

receiving the executable code and digital signature at the client computer;

preventing the executable code from executing if the digital signature of the executable code cannot be verified;

preventing the executable code from exercising privileges that are not in both (a) the authorized set of privileges from the digital certificate of the distributing authority that signed the executable code and (b) the signer-specific privilege set corresponding to the distributing authority that signed the executable code.

9. A method as recited in claim 8, further comprising:

digitally signing the digital certificate by one or more certifying authorities;

before executing the executable code, verifying the digital signature of at least one of the certifying authorities without relying on the trustworthiness of the distributing authority.

10. A method as recited in claim 8, further comprising;

certifying the trustworthiness of the distributing authority that signs the executable code with a chain of digital signatures by one or more certifying authorities;

associating the chain of digital signatures with the executable code;

before executing the executable code, tracing the chain of digital signatures to one that can be verified without relying on the trustworthiness of the distributing authority that signs the executable code.

11. A method as recited in claim 8, wherein the distributing authority that signs the executable code is a memory of a hierarchy of authorities, further comprising the following step:

creating digital certificates for members of the hierarchy, wherein the digital certificate of a particular member is signed by a higher member of the hierarchy and refers to the signed digital certificate of said higher member.

12. A method as recited in claim 8, wherein the distributing authority that signs the executable code is a memory of a hierarchy of authorities, further comprising the following steps:

creating digital certificates for members of the hierarchy, wherein the digital certificate of a particular member is signed by a higher member of the hierarchy and refers to the signed digital certificate of said higher member;

before executing the executable code, tracing the digital certificate of the distributing authority that signed the executable code to an upper member of the hierarchy of authorities whose digital signature can be verified without relying on the trustworthiness of the distributing authority that signed the executable code.

13. A method as recited in claim 8, wherein the distributing authority that signs the executable code is a memory of a hierarchy of authorities, further comprising the following steps:

creating digital certificates for members of the hierarchy, wherein the digital certificate of a particular member is signed by a higher member of the hierarchy and refers to the signed digital certificate of said higher member;

before executing the executable code, tracing the digital certificate of the distributing authority that signed the executable code to an upper member of the hierarchy of authorities whose digital signature can be verified without relying on the trustworthiness of the distributing authority that signed the executable code;

when tracing the digital certificate of the distributing authority that signed the executable code, verifying that each particular certificate's indicated authorized set of privileges is a subset of the authorized set of privileges indicated in the digital certificate of the higher member that digitally signed the particular digital certificate.

FJN 013124
SOPHOS
EXHIBIT 1004 - PAGE 0603

14. One or more computer programs stored on one or more computer-readable storage media for execution by a client computer, the one or more programs comprising the following steps:

defining signer-specific privilege sets at the client computer for different ones of a plurality of distributing authorities, each signer-specific privilege set indicating privileges allowed to executable code signed by the corresponding distributing authority;

receiving executable code and an associated privilege request code, the executable code and associated privilege request code being digitally signed by a particular one of the distributing authorities;

preventing the executable code from executing if the digital signature of the executable code and associated privilege request code cannot be verified;

preventing the executable code from executing if the privilege request code indicates privileges that are not in the signer-specific privilege set corresponding to the distributing authority that signed the executable code.

15. One or more computer programs stored on one or more computer-readable storage media as recited in claim 14, the one or more programs further comprising a step of preventing the executable code from exercising privileges that are not indicated by the privilege request code.

16. One or more computer programs stored on one or more computer-readable storage media as recited in claim 14, wherein said particular one of the distributing authorities produces a digital certificate indicating an authorized set of privileges, the one or more programs further comprising a step of preventing the executable code from exercising privileges that are not in the authorized set of privileges indicated by the digital certificate.

17. One or more computer programs stored on one or more computer-readable storage media as recited in claim 16, wherein the digital certificate is digitally signed by one or more certifying authorities, said one or more computer programs further comprising:

before executing the executable code, verifying the digital signature of at least one of the certifying authorities without relying on the trustworthiness of said particular one of the distributing authorities.

18. One or more computer programs stored on one or more computer-readable storage media as recited in claim 16, wherein the trustworthiness of said particular one of the distributing authorities is certified with a chain of digital signatures by one or more certifying authorities, the chain of digital signatures being associated with the executable code, said one or more computer programs further comprising:

before executing the executable code, tracing the chain of digital signatures to one that can be verified without relying on the trustworthiness of the distributing authority.

19. One or more computer programs stored on one or more computer-readable storage media as recited in claim 16, wherein the distributing authority that signs the executable code is a memory of a hierarchy of authorities, the members of the hierarchy having digital certificates, wherein the digital certificate of a particular member is signed by a higher member of the hierarchy and refers to the signed digital certificate of said higher member, said one or more computer programs further comprising the following step:

before executing the executable code, tracing the digital certificate of the distributing authority that signed the executable code to an upper member of the hierarchy of authorities whose digital signature can be verified without relying on the trustworthiness of the distributing authority that signed the executable code.

20. One or more computer programs stored on one or more computer-readable storage media as recited in claim 16, wherein the distributing authority that signs the executable code is a memory of a hierarchy of authorities, the members of the hierarchy having digital certificates, wherein the digital certificate of a particular member is signed by a higher member of the hierarchy and refers to the signed digital certificate of said higher member, said one or more computer programs further comprising the following step:

before executing the executable code, tracing the digital certificate of the distributing authority that signed the executable code to an upper member of the hierarchy of authorities whose digital signature can be verified without relying on the trustworthiness of the distributing authority that signed the executable code;

when tracing the digital certificate of the distributing authority that signed the executable code, verifying that each particular certificate's indicated authorized set of privileges is a subset of the authorized set of privileges indicated in the digital certificate of the higher member that digitally signed the particular digital certificate.

* * * * *

Microsoft Authenticode analyzed

Rohit Khare (*khare@pest.w3.org*)
Mon, 22 Jul 96 17:52:07 -0400

- **Messages sorted by:** [date][thread][subject][author]
- **Next message:** Rohit Khare: "Andreesen moving slooooowly to objects"
- **Previous message:** Rohit Khare: "Tim's comments on W3C appear in PCWeek"

[private w3c editorial comments expurgated]

July 22, 1996 10:00 AM ET
IE 3.0 applets will earn certification
By _Norvin Leach_ and _Michael Moeller_

In preparation for the mid-August launch of Internet Explorer 3.0, Microsoft Corp. next week will announce tools and services that let vendors digitally sign ActiveX, Java and Netscape Communications Corp. plug-in components.

As a result, users of Internet Explorer 3.0 will be able to identify the creator of an Internet-based applet before downloading it.

But for some IS managers, this approach misses the point of Internet security by a long shot. Many say they are less interested in knowing who built a component than in providing seamless protection for users, as the Java "sandbox" model does.

The Microsoft model, designed to provide users with the same level of security found in shrink-wrapped software, is based primarily on a level of trust and market pressure to keep ISVs honest.

To put the digital signature architecture in place, VeriSign Inc. and, in the future, other certificate authorities will issue digital certificates to ISVs for a $20 fee. Several hundred ActiveX controls will be digitally signed by the time Internet Explorer 3.0 ships, sources said.

But such a certificate does not authenticate the specific applet--it only certifies that the vendor has pledged not to build any malicious code into its software. "If a user downloads a buggy piece of signed code, then he will never go back to that vendor again," said Rob Price, group product manager for Internet security at Microsoft.

Beyond the credibility aspect, the signature concept raises a broader issue for some IS managers.

"Just the fact that they have to create this kind of workaround causes me

FJN 013126
SOPHOS
EXHIBIT 1004 - PAGE 0605

concern," said Eric Goldreich, information manager with Sheppard, Mullin, Richter & Hampton, a Los Angeles law firm.

Other IS managers are worried that digital signatures may add complexity to an already complicated method of trying to manage who downloads what from the Internet.

Internet Explorer 3.0 will modify a user's system files to detect digital certificates as components are downloaded. Once found, a dialog box will appear, stating where the component came from and asking if users want to continue downloading the component.

System administrations will be able to restrict users from downloading any components, and users will be able to list "trusted" companies that can load components onto their client machine without confirmation.

Security "should be something the end user isn't aware of," said Erik Goldoff, computer specialist for the Centers for Disease Control, in Atlanta. "End users don't even understand Internet busy signals today."

The issue of component security has not been widely discussed because the technology is only beginning to mature; Internet Explorer 3.0 is the first browser to apply the digital signature approach.

Two Microsoft competitors, Netscape and Sun Microsystems Inc., are adding digital signature schemes as a means of extending the functionality of software and components found on the Internet. However, officials at both companies believe digital signatures alone perpetuate a flawed model found in shrink-wrapped software.

"Digital signatures are just a part of the answer, not the whole solution," said Jeff Treuhaft, director of security at Netscape, of Mountain View, Calif. "Besides, you need to sign the code, not the vendor."

- **Next message:** Rohit Khare: "Andreesen moving slooooowly to objects"
- **Previous message:** Rohit Khare: "Tim's comments on W3C appear in PCWeek"

FJN 013127
SOPHOS
EXHIBIT 1004 - PAGE 0606

COPY

PTO/SB/17 (10-01)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
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.

FEE TRANSMITTAL for FY 2002

Patent fees are subject to annual revision.

TOTAL AMOUNT OF PAYMENT ($) 0

Complete if Known	
Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Examiner Name	Unknown
Group / Art Unit	2785
Attorney Docket No.	43426.00011

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 05-0150

Deposit Account Name: Squire, Sanders & Dempsey, L.L.P.

The Commissioner is authorized to: *(check all that apply)*
☐ Charge fee(s) indicated below ☒ Credit any overpayments
☒ Charge any additional fee(s) during the pendency of this application
☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	740	201	370	Utility filing fee	
106	330	206	165	Design filing fee	
107	510	207	255	Plant filing fee	
108	740	208	370	Reissue filing fee	
114	160	214	80	Provisional filing fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below	=	Fee Paid
Total Claims		-20 ** =	0	X		=	0
Independent Claims		-3 ** =	0	X		=	0
Multiple Dependent				X		=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	84	202	42	Independent claims in excess of 3
104	280	204	140	Multiple dependent claim, if not paid
109	84	209	42	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet.	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	400	216	200	Extension for reply within second month	
117	920	217	460	Extension for reply within third month	
118	1,440	218	720	Extension for reply within fourth month	
128	1,960	228	980	Extension for reply within fifth month	
119	320	219	160	Notice of Appeal	
120	320	220	160	Filing a brief in support of an appeal	
121	280	221	140	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive – unavoidable	
141	1,280	241	640	Petition to revive – unintentional	
142	1,280	242	640	Utility issue fee (or reissue)	
143	460	243	230	Design issue fee	
144	620	244	310	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Processing fee under 37 CFR 1.17 (q)	
126	180	126	180	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	740	246	370	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	740	249	370	For each additional invention to be examined (37 CFR § 1.129(b))	
179	740	279	370	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid SUBTOTAL (3) ($) 0

SUBMITTED BY

Complete *(if applicable)*

Name (Print/Type)	Aaron Wininger	Registration No. Attorney/Agent	45,229	Telephone	650.856.6500
Signature				Date	August 29, 2002

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.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to Commissioner for Patents, Office of Initial Patent Examination, Customer Service Center, Washington, D.C. 20231, on

Date: 8/29/02 By: _____
Aaron Wininger

In Re Application of	Shlomo Touboul	
Serial No.	09/539,667	Examiner: Unknown
Filing Date:	March 30, 2000	Group Art Unit: 2785
For:	SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES	

Office of Initial Patent Examination
Customer Service Center
Commissioner for Patents
Washington, D.C. 20231

REQUEST TO CORRECT FILING RECEIPT

1. Attached is a copy of the Official Filing Receipt as received from the U.S. Patent And Trademark Office with regard to the above-identified patent application for which issuance of a corrected Filing Receipt is respectfully requested. The errors are shown in red on the Filing Receipt as well as described below.

2. There is an error in that the following data is:

- ☐ incorrectly entered
  and/or
- ☒ omitted
- ☐ Applicant's name
- ☐ Applicant's address
- ☐ Title
- ☐ Filing Date
- ☐ Serial Number
- ☐ Foreign Application Reference
- ☐ Attorney Docket No.
- ☒ Other – Continuing Data As Claimed by Applicant

in that the filing receipt should read as follows:

Continuing Data as Claimed by Applicant

THIS APPLICATION IS A CON OF 08/964,388	**11/06/1997**
WHICH CLAIMS BENEFIT OF 60/030,639	**11/08/1996**

3. Please issue a corrected Filing Receipt rectifying the above errors.

If for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No. **05-0150**.

Date: August 29, 2002

Respectfully submitted,

Squire, Sanders & Dempsey L.L.P.
600 Hansen Way
Palo Alto, CA 94304-1043
Telephone: 650-856-6500
Facsimile: 650-843-8777

By: _____
Aaron Wininger
Attorney for Applicant
Reg. No. 45,229

FJN 013130
SOPHOS
EXHIBIT 1004 - PAGE 0609

FILING RECEIPT

OC000000005176721

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: ASSISTANT SECRETARY AND
COMMISSIONER OF PATENT AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	DRAWINGS	TOT CLAIMS	IND CLAIMS
09/539,667	03/30/2000	2785	402	40492.00011	10	22	4

Graham & James LLP
600 Hansen Way
Palo Alto, CA 94304-1043

Date Mailed: 06/14/2000

Receipt is acknowledged of this nonprovisional Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. 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 write to the Office of Initial Patent Examination's Customer Service Center. 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 PTO processes the reply to the Notice, the PTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

Applicant(s)

Shlomo Touboul, Kefar-haim, ISRAEL;

Continuing Data as Claimed by Applicant

~~THIS APPLN CLAIMS BENEFIT OF 60/030,699 11/07/1996~~
THIS Application is a CON of 08/964,388 11/06/1997 WHICH CLAIMS Benefit of 60/030,639 11/08/1996

Foreign Applications

If Required, Foreign Filing License Granted 06/14/2000

**** SMALL ENTITY ****

Title

System and method for protecting a computer and a network from hostile downloadables

Preliminary Class

713

Data entry by : BURNS, DORIS **Team :** OIPE **Date:** 06/14/2000

DATES ENTERED: No Action

JUN 20 2000

CALENDARED

BY HD
ATTORNEY
GRAHAM & JAMES (PA) IP DEPT.

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 CRF 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 36 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 Office of Export Administration, Department of Commerce (15 CFR 370.10 (j)); 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).

PLEASE NOTE the following information about the Filing Receipt:

- The articles such as "**a**," "**an**" and "**the**" are not included as the first words in the title of an application. They are considered to be unnecessary to the understanding of the title.
- The words "**new**," "**improved**," "**improvements in**" or "**relating to**" are not included as first words in the title of an application because a patent application, by nature, is a new idea or improvement.
- The title may be truncated if it consists of more than 600 characters (letters and spaces combined).
- The docket number allows a maximum of 25 characters.
- If your application was submitted under 37 CFR 1.10, your filing date should be the "date in" found on the Express Mail label. If there is a discrepancy, you should submit a request for a corrected Filing Receipt along with a copy of the Express Mail label showing the "date in."

Any corrections that may need to be done to your Filing Receipt should be directed to:

Assistant Commissioner for Patents
Office of Initial Patent Examination
Customer Service Center
Washington, DC 20231

NO DOCKETING REQUIRED

DATES ENTERED _____

OCT 0 4 2001

CALENDARED

BY _____

ATTORNEY _____

SQUIRE, SANDERS & DEMPSEY

Date Mailed: September 17, 2001 | By: MAS/say | PTO DATE STAMP:

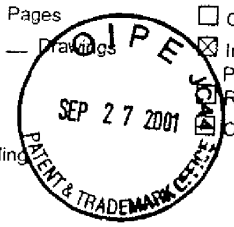
Serial No.: 09/539,667 | Docket No.: 43426.00011

Applicant(s): Shlomo Touboul

Title: SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

The following has been received in the U.S. Patent Office on the date stamped hereon:

- ☐ Patent Application __ Pages __ Claims
- ☐ Drawings Formal/Informal _____ Sheets
- ☐ General Authorization / Request to Petition for Extensions of Time
- ☐ Oath/Declaration/Power of Attorney
- ☐ Assignment & Recordation Cover Sheet
- ☐ Verified Statement Claiming Small Entity Status
- ☐ Continued Prosecution Application (§1.53(d) CPA - in duplicate)
- ☐ Provisional Application _____ Pages
- ☐ Design Application __ Pages __ Drawings
- ☐ Status Letter
- ☐ Check No. for $
- ☒ Certificate(s) of First Class Mailing
- ☐ Amendment/Response
- ☐ Petition for Extension of Time
- ☒ Transmittal Form
- ☒ Fee Transmittal for FY 2001 (in duplicate)
- ☐ Appeal Brief (in triplicate)
- ☐ Issue Fee Transmittal with PTO-85b Drawings
- ☐ Copy of PTO-1533, Notice to File Missing Parts
- ☒ Info. Disclosure Statement (2 pages) & PTO-1449 (2 pages) w/ 43 References
- ☐ Request to Correct Filing Receipt
- ☐ Check No. for $



Date Mailed: September 17, 2001 | By: MAS/say | PTO DATE STAMP:

Serial No.: 09/539,667 | Docket No.: 43426.00011

Applicant(s): Shlomo Touboul

Title: SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

The following has been received in the U.S. Patent Office on the date stamped hereon:

- ☐ Patent Application __ Pages __ Claims
- ☐ Drawings Formal/Informal _____ Sheets
- ☐ General Authorization / Request to Petition for Extensions of Time
- ☐ Oath/Declaration/Power of Attorney
- ☐ Assignment & Recordation Cover Sheet
- ☐ Verified Statement Claiming Small Entity Status
- ☐ Continued Prosecution Application (§1.53(d) CPA - in duplicate)
- ☐ Provisional Application _____ Pages
- ☐ Design Application __ Pages __ Drawings
- ☐ Status Letter
- ☐ Check No. for $
- ☒ Certificate(s) of First Class Mailing
- ☐ Amendment/Response
- ☐ Petition for Extension of Time
- ☒ Transmittal Form
- ☒ Fee Transmittal for FY 2001 (in duplicate)
- ☐ Appeal Brief (in triplicate)
- ☐ Issue Fee Transmittal with PTO-85b Drawings
- ☐ Copy of PTO-1533, Notice to File Missing Parts
- ☒ Info. Disclosure Statement (2 pages) & PTO-1449 (2 pages) w/ 43 References
- ☐ Request to Correct Filing Receipt
- ☐ Check No. for $

U.S DEPARTMENT OF COMMERCE
PATENT/TRADEMARK OFFICE
WASHINGTON, D.C. 20231

PALO ALTO

Squire, Sanders & Dempsey L.L.P.
600 Hansen Way, Suite 100
Palo Alto, CA 94304-1043

Please type a plus sign (+) inside this box → [+]

PTO/SB/21 (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
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.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Group Art Unit	2785
Examiner Name	Unknown
Attorney Docket Number	43426.00011

ENCLOSURES *(check all that apply)*

- ☒ Fee Transmittal Form
  - ☐ Fee Attached
  - ☒ Deposit Account Authorization on Fee Transmittal Form
- ☐ Amendment / Response
  - ☐ After Final
- ☐ Signed Oath/Declaration
- ☐ Extension of Time Request
- ☒ Return Postcard
- ☒ Information Disclosure Statement (2 pages) & PTO Form 1449 (2 pages)
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts
- ☐ Response to Incomplete Application
- ☐ Assignment & Cover Sheet *(for an Application)*
- ☐ Drawing(s) _____ sheets
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance Communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) *(please identify below)*: **43 References**

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Marc A. Sockol, Reg. No. 40,823 Squire, Sanders & Dempsey, L.L.P. 600 Hansen Way Palo Alto, CA 94304-1043
Signature	M A. Sockol
Date	September 17, 2001

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231 on this date: September 17, 2001

Typed or printed name	Sandy Yi		
Signature	Sandy Yi	Date	September 17, 2001

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be send to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

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.

FEE TRANSMITTAL for FY 2001

Patent fees are subject to annual revision.

TOTAL AMOUNT OF PAYMENT ($) 0

Complete If Known	
Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Examiner Name	Unknown
Group / Art Unit	2785
Attorney Docket No.	43426.00011

METHOD OF PAYMENT (check one)

1. ☒ The Commissioner is hereby authorized to charge indicated fees and credit any over payments to:

Deposit Account Number: 05-0150

Deposit Account Name: Squire, Sanders & Dempsey, L.L.P.

☒ Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17

☒ Applicant claims small entity status. See 37 CFR 1.27

2. ☐ Payment Enclosed:

☐ Check ☐ Credit card ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	710	201	355	Utility filing fee	
106	320	206	160	Design filing fee	
107	490	207	245	Plant filing fee	
108	710	208	355	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below	=	Fee Paid
Total Claims		-20 =	0	X		=	0
Independent Claims		-3 =	0	X		=	0
Multiple Dependent				X		=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	80	202	40	Independent claims in excess of 3
104	270	204	135	Multiple dependent claim, if not paid
109	80	209	40	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet.	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	390	216	195	Extension for reply within second month	
117	890	217	445	Extension for reply within third month	
118	1,390	218	695	Extension for reply within fourth month	
128	1,890	228	945	Extension for reply within fifth month	
119	310	219	155	Notice of Appeal	
120	310	220	155	Filing a brief in support of an appeal	
121	270	221	135	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive – unavoidable	
141	1,240	241	620	Petition to revive – unintentional	
142	1,240	242	620	Utility issue fee (or reissue)	
143	440	243	220	Design issue fee	
144	600	244	300	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	130	123	130	Petitions related to provisional applications	
126	180	126	180	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	710	246	355	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	710	249	355	For each additional invention to be examined (37 CFR § 1.129(b))	
179	710	279	355	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid SUBTOTAL (3) ($) 0

SUBMITTED BY

					Complete (if applicable)
Name (Print/Type)	Marc A. Sockol	Registration No. Attorney/Agent	40,823	Telephone	650.856.6500
Signature				Date	September 17, 2001

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.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

COPY

PTO/SB/17 (11-00)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
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.

FEE TRANSMITTAL for FY 2001

Patent fees are subject to annual revision.

TOTAL AMOUNT OF PAYMENT ($) 0

Complete If Known	
Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Examiner Name	Unknown
Group / Art Unit	2785
Attorney Docket No.	43426.00011

METHOD OF PAYMENT (check one)

1. ☒ The Commissioner is hereby authorized to charge indicated fees and credit any over payments to:

Deposit Account Number: 05-0150

Deposit Account Name: Squire, Sanders & Dempsey, L.L.P.

☒ Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17

☒ Applicant claims small entity status. See 37 CFR 1.27

2. ☐ Payment Enclosed:

☐ Check ☐ Credit card ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	710	201	355	Utility filing fee	
106	320	206	160	Design filing fee	
107	490	207	245	Plant filing fee	
108	710	208	355	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below	=	Fee Paid
Total Claims		-20	0	X		=	0
Independent Claims		-3	0	X		=	0
Multiple Dependent				X		=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	80	202	40	Independent claims in excess of 3
104	270	204	135	Multiple dependent claim, if not paid
109	80	209	40	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet.	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	390	216	195	Extension for reply within second month	
117	890	217	445	Extension for reply within third month	
118	1,390	218	695	Extension for reply within fourth month	
128	1,890	228	945	Extension for reply within fifth month	
119	310	219	155	Notice of Appeal	
120	310	220	155	Filing a brief in support of an appeal	
121	270	221	135	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive – unavoidable	
141	1,240	241	620	Petition to revive – unintentional	
142	1,240	242	620	Utility issue fee (or reissue)	
143	440	243	220	Design issue fee	
144	600	244	300	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	130	123	130	Petitions related to provisional applications	
126	180	126	180	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	710	246	355	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	710	249	355	For each additional invention to be examined (37 CFR § 1.129(b))	
179	710	279	355	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid SUBTOTAL (3) ($) 0

SUBMITTED BY

Complete *(if applicable)*

Name (Print/Type)	Marc A. Sockol	Registration No. Attorney/Agent	40,823	Telephone	650.856.6500
Signature				Date	September 17, 2001

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.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

PATENT
Attorney Docket No.: 43426.00011

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF MAILING

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to Commissioner for Patents, Washington, D.C. 20231, on

Date: 9/17/01 By: Sandy Yi
Sandy Yi

In re Application of:			
	Shlomo Touboul	Examiner:	Unknown
Serial No.:	09/539,667	Art Unit:	2785
Filed:	March 30, 2000		
Title:	SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES		

Commissioner for Patents
Washington, D.C. 20231

INFORMATION DISCLOSURE STATEMENT PURSUANT TO 37 C.F.R. §§1.97-1.98

Sir:

In accordance with the duty of disclosure under 37 C.F.R. §1.56 and pursuant to 37 C.F.R. §§1.97-1.98, Applicant hereby notifies the U.S. Patent and Trademark Office of the references listed on the attached Form PTO-1449. One copy of each cited reference is submitted herewith.

The submission of the listed documents is not intended as an admission that any such document constitutes prior art against the claims of the present application. Applicant reserves the right to dispute any of the listed documents as prior art during examination. Furthermore, Applicant does not waive any right to take any action that would be appropriate to antedate or otherwise remove any listed document as a competent reference against the claims of the present application. The submission of this Information Disclosure Statement is not to be construed as a representation that a search has been made or that no other material information may exist.

FJN 013138
SOPHOS
EXHIBIT 1004 - PAGE 0617

The Examiner is requested to initial the enclosed Form PTO-1449 and return a copy thereof to the undersigned.

The present Information Disclosure Statement is being filed before receiving the first Office Action. Therefore, no certification under 37 C.F.R. §1.97(e) or fee under 37 C.F.R. §1.17(p) is required.

However, if for any reason an insufficient fee has been paid, please charge the insufficiency to Deposit Account No. **05-0150**.

Date: September 17, 2001

Respectfully submitted,

Squire, Sanders & Dempsey L.L.P.
600 Hansen Way
Palo Alto, CA 94304-1043
Telephone (650) 856-6500
Facsimile (650) 843-8777

Marc A. Sockol
Attorney for Applicant
Reg. No. 40,823

FJN 013139
SOPHOS
EXHIBIT 1004 - PAGE 0618

Please type a plus sign (+) inside this box [+]

PTO/SB/08A (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Group Art Unit	2785
Examiner Name	Unknown
Attorney Docket Number	43426.00011

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		5,077,677		John H. Murphy, et al.	12-31-1991	
		5,359,659		Doren Rosenthal	10-25-1994	
		5,361,359		Homayoon Tajalli, et al.	11-01-1994	
		5,485,409		Sarbari Gupta, et al.	01-16-1996	
		5,485,575		David M. Chess, et al.	01-16-1996	
		5,572,643		David H. Judson	11-05-1996	
		5,606,668		Gil Shwed	02-25-1997	
		5,623,600		Shuang Ji, et al.	04-22-1997	
		5,638,446		Aviel D. Rubin	06-10-1997	
		5,692,047		Charles E. McManis	11-25-1997	
		5,692,124		James M. Holden, et al.	11-25-1997	
		5,720,033		Umesh Deo	02-17-1998	
		5,724,425		Sheue-Ling Chang, et al.	03-03-1998	
		5,740,248		Helmut Fieres, et al.	04-14-1998	
		5,761,421		Arthur A. van Hoff, et al.	06-02-1998	
		5,765,205		Franklin Charles Breslau, et al.	06-09-1998	
		5,784,459		Murthy Devarakonda, et al.	07-21-1998	
		5,796,952		Owen Davis, et al.	08-18-1998	
		5,805,829		Geoffrey Alexander Cohen, et al.	09-08-1998	
		5,832,208		Chia-Hwang Chen, et al.	11-03-1998	
		5,850,559		Michael F. Angelo, et al.	12-15-1998	
		5,859,966		Kenneth John Hayman, et al.	01-12-1999	
		5,864,683		William E. Boebert, et al.	01-26-1999	
		5,892,904		Robert G. Atkinson, et al.	04-06-1999	
		5,951,698		Eva Y. Chen, et al.	09-14-1999	
		5,956,481		James E. Walsh, et al.	09-21-1999	
		5,974,549		Gilad Golan	10-26-1999	
		5,983,348		Shuang Ji	11-09-1999	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Office[3]	Number[4]	Kind Code[5] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

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.

[1] Unique citation designation number. [2] See attached Kinds of U.S. Patent Documents. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark hee if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	09/539,667
Filing Date	March 30, 2000
First Named Inventor	Shlomo Touboul
Group Art Unit	2785
Examiner Name	Unknown
Attorney Docket Number	43426.00011

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials *	Cite No.[1]	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, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		JIM K. OMURA, "Novel Applications of Cryptography in Digital Communications", IEEE Communications Magazine, May, 1990, pages 21-29.	
		OKAMOTO, E. et al., "ID-Based Authentication System For Computer Virus Detection", IEEE/IEE Electronic Library online, Electronics Letters, Vol. 26, Issue 15, ISSN 0013-5194, July 19, 1990, Abstract and pages 1169-1170. URL: http://iel.ihs.com:80/cgi-bin/iel_cgi?se...2ehts%26ViewTemplate%3ddocview%5fb%2ehts.	
		IBM AntiVirus User's Guide Version 2.4, International Business Machines Corporation, November 15, 1995, page 6-7.	
		NORVIN LEACH et al, "IE 3.0 Applets Will Earn Certification", PC Week, Vol. 13, No. 29, July 22, 1996, 2 pages.	
		"Finjan Software Releases SurfinBoard, Industry's First JAVA Security Product For the World Wide Web", Article published on the Internet by Finjan Software Ltd., July 29, 1996, 1 page.	
		"Powerful PC Security for the New World of Java™ and Downloadables, Surfin Shield™" Article published on the Internet by Finjan Software Ltd., 1996, 2 Pages.	
		Microsoft® Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet", Microsoft Corporation, October 1996, including Abstract, Contents, Introduction and pages 1-10.	
		"Finjan Announces a Personal Java™ Firewall For Web Browsers - the SurfinShield™ 1.6 (formerly known as SurfinBoard)", Press Release of Finjan Releases SurfinShield 1.6, October 21, 1996, 2 pages.	
		Company Profile "Finjan - Safe Surfing, The Java Security Solutions Provider" Article published on the Internet by Finjan Software Ltd., October 31, 1996, 3 pages.	
		"Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0" Las Vegas Convention Center/Pavilion 5 P5551, November 18, 1996, 3 pages.	
		"Java Security: Issues & Solutions" Article published on the Internet by Finjan Software Ltd., 1996, 8 pages.	
		"Products" Article published on the Internet, 7 pages.	
		MARK LaDUE, "Online Business Consultant: Java Security: Whose Business Is It?" Article published on the Internet, Home Page Press, Inc. 1996, 4 pages.	
		Web Page Article "Frequently Asked Questions About Authenticode", Microsoft Corporation, last updated February 17, 1997, Printed December 23, 1998. URL: http://www.microsoft.com/workshop/security/authcode/signfaq.asp#9, pages 1-13.	
		ZHANG, X.N., "Secure Code Distribution", IEEE/IEE Electronic Library online, Computer, Vol. 30, Issue 6, June, 1997, Pages: 76-79.	

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.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

FILING RECEIPT

OC000000005176721

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: ASSISTANT SECRETARY AND
COMMISSIONER OF PATENT AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NUMBER	FILING DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	DRAWINGS	TOT CLAIMS	IND CLAIMS
09/539,667	03/30/2000	2785	402	40492.00011	10	22	4

Graham & James LLP
600 Hansen Way
Palo Alto, CA 94304-1043

Date Mailed: 06/14/2000

Receipt is acknowledged of this nonprovisional Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. 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 write to the Office of Initial Patent Examination's Customer Service Center. 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 PTO processes the reply to the Notice, the PTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

Applicant(s)

Shlomo Touboul, Kefar-haim, ISRAEL;

Continuing Data as Claimed by Applicant

THIS APPLN CLAIMS BENEFIT OF 60/030,699 11/07/1996

Foreign Applications

If Required, Foreign Filing License Granted 06/14/2000

**** SMALL ENTITY ****

DATES ENTERED: No Action

JUN 20 2000

CALENDARED

BY MD
ATTORNEY
GRAHAM & JAMES (PA) IP DEPT.

Title

System and method for protecting a computer and a network from hostile downloadables

Preliminary Class

713

Data entry by : BURNS, DORIS **Team :** OIPE **Date:** 06/14/2000

FJN 013142
SOPHOS
EXHIBIT 1004 - PAGE 0621

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 CRF 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 36 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 Office of Export Administration, Department of Commerce (15 CFR 370.10 (j)); 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).

PLEASE NOTE the following information about the Filing Receipt:

- The articles such as **"a," "an"** and **"the"** are not included as the first words in the title of an application. They are considered to be unnecessary to the understanding of the title.
- The words **"new," "improved," "improvements in"** or **"relating to"** are not included as first words in the title of an application because a patent application, by nature, is a new idea or improvement.
- The title may be truncated if it consists of more than 600 characters (letters and spaces combined).
- The docket number allows a maximum of 25 characters.
- If your application was submitted under 37 CFR 1.10, your filing date should be the "date in" found on the Express Mail label. If there is a discrepancy, you should submit a request for a corrected Filing Receipt along with a copy of the Express Mail label showing the "date in."

Any corrections that may need to be done to your Filing Receipt should be directed to:

Assistant Commissioner for Patents
Office of Initial Patent Examination
Customer Service Center
Washington, DC 20231

FJN 013143
SOPHOS
EXHIBIT 1004 - PAGE 0622

DATES ENTERED: No Action

APR 11 2000

CALENDARED

BY MD

ATTORNEY

GRAHAM & JAMES (PA) IP DEPT.

Date Mailed: March 30, 2000 | By: MAS/md | PTO DATE STAMP:

Serial No.: Unassigned | Docket No.: 40492.00011

Applicant(s): Shlomo Touboul

Title: System And Method For Protecting A Computer And A Network From Hostile Downloadables

The following has been received in the U.S. Patent Office on the date stamped hereon:

- ☒ Patent Application 26 Pages 22 Claims (Cont.)
- ☒ Drawings Formal 10 Sheets
- ☒ General Authorization / Request to Petition for Extensions of Time
- ☒ Oath/Declaration/Power of Attorney (copy)
- ☒ Assignment & Recordation Cover Sheet (copy)
- ☒ Verified Statement Claiming Small Entity Status (copy)
- ☐ Continued Prosecution Application (§1.53(d) CPA - in duplicate)
- ☐ Provisional Application ____ Pages
- ☐ Design Application __ Pages __ Drawings
- ☐ Status Letter
- ☐ Check No. for $
- ☐ Other:
- ☒ Express Mail # EL515155991US
- ☐ Amendment/Response
- ☐ Petition for Extension of Time
- ☒ Transmittal Letter
- ☐ Notice of Appeal
- ☐ Appeal Brief (in triplicate)
- ☐ Issue Fee Transmittal with PTO-85b Drawings
- ☐ Copy of PTO-1533, Notice to File Missing Parts
- ☐ Info. Disclosure Statement & PTO-1449/Refs
- ☐ Request to Correct Filing Receipt
- ☒ Check No. 24243 for $402.00

jc511 U.S. PTO
09/539667
03/30/00

POST OFFICE TO ADDRESSEE

EXPRESS MAIL
UNITED STATES POSTAL SERVICE™

EL515155991US

EL515155991US

SEE REVERSE SIDE FOR SERVICE GUARANTEE AND LIMITS ON INSURANCE COVERAGE

Customer Copy
Label 11-F July 1997

ORIGIN (POSTAL USE ONLY)

PO ZIP Code	Day of Delivery	Flat Rate Envelope
94306	☐ Next ☑ Second	☐
Date In: Mo. 3 Day 30 Year 00	☐ 12 Noon ☐ 3 PM	Postage: $ 15.25
Time In: 5:02 ☐ AM ☑ PM	Military: ☐ 2nd Day ☐ 3rd Day	Return Receipt Fee
Weight: lbs. 11 ozs.	Int'l Alpha Country Code	COD Fee / Insurance Fee
No Delivery: ☐ Weekend ☐ Holiday	Acceptance Clerk Initials: JO	Total Postage & Fees: $ 15.25

METHOD OF PAYMENT:
Express Mail Corporate Acct. No: X940244
Federal Agency Acct. No. or Postal Service Acct. No:

☐ WAIVER OF SIGNATURE (Domestic Only): Additional merchandise insurance is void if waiver of signature is requested. I wish delivery to be made without obtaining signature of addressee or addressee's agent (if delivery employee judges that article can be left in secure location) and I authorize delivery employee's signature constitutes proof of delivery.
NO DELIVERY ☐ Weekend ☐ Holiday

FROM: (PLEASE PRINT) PHONE ( )
GRAHAM & JAMES LLP 40492.00011
600 HANSEN WAY STE 100
PALO ALTO CA 94304-1043

TO: (PLEASE PRINT) PHONE ( )
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON DC 20231-9999
BOX - NEW PATENT APPLICATION

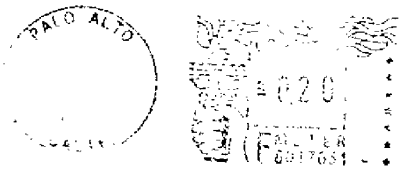
PRESS HARD. You are making 3 copies. FOR PICKUP OR TRACKING CALL 1-800-222-1811 www.usps.gov EMS

Date Mailed: March 30, 2000	By: MAS/md	PTO DATE STAMP:
Serial No.: Unassigned		Docket No.: 40492.00011
Applicant(s): Shlomo Touboul		
Title: System And Method For Protecting A Computer And A Network From Hostile Downloadables		

The following has been received in the U.S. Patent Office on the date stamped hereon:

- ☒ Patent Application 26 Pages 22 Claims (Cont.)
- ☒ Drawings Formal 10 Sheets
- ☒ General Authorization / Request to Petition for Extensions of Time
- ☒ Oath/Declaration/Power of Attorney (copy)
- ☒ Assignment & Recordation Cover Sheet (copy)
- ☒ Verified Statement Claiming Small Entity Status (copy)
- ☐ Continued Prosecution Application (§1.53(d) CPA - in duplicate)
- ☐ Provisional Application ____ Pages
- ☐ Design Application __ Pages __ Drawings
- ☐ Status Letter
- ☐ Check No. for $
- ☐ Other:
- ☒ Express Mail # EL515155991US
- ☐ Amendment/Response
- ☐ Petition for Extension of Time
- ☒ Transmittal Letter
- ☐ Notice of Appeal
- ☐ Appeal Brief (in triplicate)
- ☐ Issue Fee Transmittal with PTO-85b Drawings
- ☐ Copy of PTO-1533, Notice to File Missing Parts
- ☐ Info. Disclosure Statement & PTO-1449/Refs
- ☐ Request to Correct Filing Receipt
- ☒ Check No. 24243 for $402.00

U.S. DEPARTMENT OF COMMERCE
PATENT/TRADEMARK OFFICE
WASHINGTON, D.C. 20231



Graham & James LLP
600 Hansen Way
Palo Alto, CA 94304-1043

131/200701.01

GRAHAM & JAMES LLP

24243

004032 40492 00011 42 402.00 Patent & T Filing of a Continued Patent Application

03/30/00 402.00 24243

GRAHAM & JAMES LLP
ATTORNEYS AT LAW
GENERAL ACCOUNT
600 HANSEN WAY
PALO ALTO, CA 94306

24243

90-4153
1211

PAY FOUR HUNDRED TWO AND 00/100 DOLLARS

DATE 03/30/00

MID-PENINSULA BANK
415-323-5150
400 COWPER STREET
PALO ALTO, CA 94301

PAY EXACTLY *$*****402.00

TO THE ORDER OF Assistant Commissioner of Patents

GRAHAM & JAMES LLP

NOT NEGOTIABLE

TWO SIGNATURES REQUIRED FOR $2,500 AND ABOVE

Express Mail Label No. EL515 0911

UTILITY PATENT APPLICATION TRANSMITTAL
(Small Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No. 40492.00011

Total Pages in this Submission

TO THE ASSISTANT COMMISSIONER FOR PATENTS
Box Patent Application
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

and invented by:

Shlomo Touboul

If a CONTINUATION APPLICATION, *check appropriate box and supply the requisite information:*

☒ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: **08/964,388**

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Enclosed are:

Application Elements

1. ☒ Filing fee as calculated and transmitted as described below
2. ☒ Specification having **26** pages and including the following:
   - a. ☒ Descriptive Title of the Invention
   - b. ☒ Cross References to Related Applications *(if applicable)*
   - c. ☐ Statement Regarding Federally-sponsored Research/Development *(if applicable)*
   - d. ☐ Reference to Microfiche Appendix *(if applicable)*
   - e. ☒ Background of the Invention
   - f. ☒ Brief Summary of the Invention
   - g. ☒ Brief Description of the Drawings *(if drawings filed)*
   - h. ☒ Detailed Description
   - i. ☒ Claim(s) as Classified Below
   - j. ☒ Abstract of the Disclosure

FJN 013148
SOPHOS
EXHIBIT 1004 - PAGE 0627

UTILITY PATENT APPLICATION TRANSMITTAL
(Small Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No. 40492.00011
Total Pages in this Submission

Application Elements (Continued)

3. ☒ Drawing(s) *(when necessary as prescribed by 35 USC 113)*
   a. ☒ Formal b. ☐ Informal Number of Sheets 10

4. ☒ Oath or Declaration
   a. ☐ Newly executed *(original or copy)* ☐ Unexecuted
   b. ☒ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*
   c. ☒ With Power of Attorney ☐ Without Power of Attorney
   d. ☐ *DELETION OF INVENTOR(S)*
   Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. 1.63(d)(2) and 1.33(b).

5. ☒ Incorporation By Reference *(usable if Box 4b is checked)*
   The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ☐ Computer Program in Microfiche

7. ☐ Genetic Sequence Submission *(if applicable, all must be included)*
   a. ☐ Paper Copy
   b. ☐ Computer Readable Copy
   c. ☐ Statement Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

8. ☒ Assignment Papers *(cover sheet & documents)*

9. ☐ 37 CFR 3.73(b) Statement *(when there is an assignee)*

10. ☐ English Translation Document *(if applicable)*

11. ☐ Information Disclosure Statement/PTO-1449 ☐ Copies of IDS Citations

12. ☐ Preliminary Amendment

13. ☒ Acknowledgment postcard

14. ☒ Certificate of Mailing
    ☐ First Class ☒ Express Mail *(Specify Label No.):* EL515155991US

FJN 013149
SOPHOS
EXHIBIT 1004 - PAGE 0628

UTILITY PATENT APPLICATION TRANSMITTAL
(Small Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
40492.00011
Total Pages in this Submission

Accompanying Application Parts (Continued)

15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*

16. ☒ Small Entity Statement(s) - Specify Number of Statements Submitted: 1

17. ☒ Additional Enclosures *(please identify below):*

General Authorization/Request to Petition for Extensions of Time

Fee Calculation and Transmittal

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra		Rate	Fee
Total Claims	22	- 20 =	2	x	$9.00	$18.00
Indep. Claims	4	- 3 =	1	x	$39.00	$39.00
Multiple Dependent Claims (check if applicable) ☐						$0.00
					BASIC FEE	$345.00
OTHER FEE *(specify purpose)*						$0.00
					TOTAL FILING FEE	$402.00

☒ A check in the amount of **$402.00** to cover the filing fee is enclosed.

☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. **05-0150** as described below. A duplicate copy of this sheet is enclosed.

- ☐ Charge the amount of as filing fee.
- ☒ Credit any overpayment.
- ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

Dated: **March 30, 2000**

Signature

Marc A. Sockol, Reg. No. 40,823
Attorney for Applicant
Graham & James LLP
600 Hansen Way
Palo Alto, CA 94304-1043
Tel: (650) 856-6500
Fax: (650) 856-3619

cc:

COMBINED DECLARATION FOR PATENT APPLICATION & POWER OF ATTORNEY	DOCKET NO.: 40492.00002

As a below named inventor, I hereby declare that:

The information given herein is true;

My residence, post office address and citizenship are as stated below next to my name;
I BELIEVE I AM THE ORIGINAL, FIRST AND SOLE INVENTOR (if only one name is listed below) OR AN ORIGINAL, FIRST AND JOINT INVENTOR (if poural names are listed below) OF THE SUBJECT MATTER WHICH IS CLAIMED AND FOR WHICH A PATENT IS SOUGHT ON THE INVENTION ENTITLED:

SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

the specification of which (check only one item below):

☐ is attached hereto;

☒ was filed on 11/05/97 United States
Application Serial No. 08/964,388
and was amended on _____ (if applicable).

☐ was filed on _____ as PCT International
Application Serial No. _____
and was amended under PCT Article 19 _____ (if applicable).

I hereby state that I have reviewed and understand the content 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 the examination of this application in accordance with Title 37, Code of Federal Regulations Section 1.56(a).

I hereby claim the benefit under Title 35, United States, §119(a) of any United States provisional application(s) listed below.

60/030,699 (Application Number) November 8, 1996 (Filing Date)

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119 of any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America having a filing date before that of the application(s) on which priority is claimed.

FOREIGN APPLICATION(S), IF ANY, FILED WITHIN 12 (6 if a Design) MONTHS PRIOR TO THE FILING DATE OF THIS APPLICATION THE PRIORITY OF WHICH WHERE PERMITTED IS HEREBY CLAIMED UNDER 35 U.S.C. SEC. 119.

COUNTRY	APPLICATION OF NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)	PRIORITY CLAIMED	
				yes	
				yes	
				yes	

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) or PCT international application(s) designating the United States of America that is/are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in that/those prior application(s) in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application(s) and the national or PCT international filing date of this application.

131/125258.01.00
033198/1111/40492.00002

1

COPY

COMBINED DECLARATION (PAT APPLICATION & POWER OF ATTORNEY - Combi			ATTORNEY'S DOCKET NO. 40492.00002
U.S. APPLICATION NO.	U.S. FILING DATE	PATENTED	PENDING / ABANDONED
PCT APPLICATIONS DESIGNATING THE U.S.			
PCT APPLICATION NO.	PCT FILING DATE	U.S. SERIAL NUMBERS	

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or Agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.
David L. Fehrman, Reg. No. 28,600; David L. Henty, Reg. No. 31,323; William J. Robinson, Reg. No. 29,430; Stuart L. Merkadeau, Reg. No. 33,262; David B. Abel Reg. No. 32,394; Hisako Muramatsu, Reg. No. 34,955; Brian M. Berliner, Reg. No. 34,549; David J. Meyer, Reg. No. 33,425; Vincent J. Belusko, Reg. No. 30,820; Minda Schechter, Reg. No. 38,296; William G. Anderson, Reg. No. 27,851; Victor De Gyarfas, Reg. No. 40,583; Dennis R. Gallagher, Reg. No. 42,563; Jonathan L. Peiss, Reg. No. 40,770; Wayne Smith, Reg. No. 42,160; Lawrence W. Granatelli, Reg. No. 32,228; Laura A. Majeruz, Reg. No. 33,417; Joseph K. Hollinger, Reg. No. 40,649; Jonathan T. Kaplan, Reg. No. 38,935; Marc A. Sockol, Reg. No. 40,823 ; Ian Cartier, Reg. No. 38,406; Linda Beach, Reg. No. 36,446.

Send correspondence to	GRAHAM & JAMES LLP 600 Hansen Way Palo Alto, CA 94304-1043	Direct Phone Calls To: Lawrence Granatelli - 650-856-6500

1	FULL NAME OF INVENTOR	LAST NAME TOUBOUL	FIRST NAME SHLOMO	MIDDLE NAME –	
	RESIDENCE & CITIZENSHIP	CITY KEFAR-HAIM	STATE OR FOREIGN COUNTRY ISRAEL	COUNTRY OF CITIZENSHIP ISRAEL	
	POST OFFICE ADDRESS	STREET –	CITY KEFAR-HAIM	STATE OR COUNTRY ISRAEL	ZIP CODE 42945
2	FULL NAME OF INVENTOR	LAST NAME	FIRST NAME	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP	
	POST OFFICE ADDRESS	STREET	CITY	STATE OR COUNTRY	ZIP CODE
3	FULL NAME OF INVENTOR	LAST NAME	FIRST NAME	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY	STATE OR FOREIGN COUNTRY	COUNTRY OF CITIZENSHIP	
	POST OFFICE ADDRESS	STREET	CITY	STATE OR COUNTRY	ZIP CODE

I further 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 issuing thereon.

SIGNATURE OF INVENTOR 1	SIGNATURE OF INVENTOR 2	SIGNATURE OF INVENTOR 3	SIGNATURE OF INVENTOR 4
DATE 13.5.98	DATE	DATE	DATE

131/125259.01.00
033198/1111/40492.00002

TOTAL P.07

TOTAL P.08

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) AND 1.27 (c)) - SMALL BUSINESS CONCERN

Docket No. 40492.00002

Serial No.	Filing Date	Patent No.	Issue Date
08/964,388	November 6, 1997	Unassigned	Unassigned

Applicant/ Patentee: Shlomo Touboul

Invention: System and Method for Protecting aComputer and a Network from Hostile Downloadables

I hereby declare that I am:

- ☐ the owner of the small business concern identified below:
- ☒ an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF CONCERN: Finjan Software, Ltd.
ADDRESS OF CONCERN: Netanya, Israel 42504

I hereby declare that the above-identified small business concern qualifies as a small business concern as defined in 13 CFR 121.3-18, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees under Section 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the above identified invention described in:

- ☐ the specification filed herewith with title as listed above.
- ☒ the application identified above.
- ☐ the patent identified above.

If the rights held by the above-identified small business concern are not exclusive, each individual, concern or organization having rights to the invention is listed on the next page and no rights to the invention are held by any person, other than the inventor, who could not qualify as an independent inventor under 37 CFR 1.9(c) or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

COPY

Copyright 1994 Logistech

Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

☒ no such person, concern or organization exists.
☐ each such person, concern or organization is listed below.

FULL NAME _____
ADDRESS _____
☐ Individual ☐ Small Business Concern ☐ Nonprofit Organization

FULL NAME _____
ADDRESS _____
☐ Individual ☐ Small Business Concern ☐ Nonprofit Organization

FULL NAME _____
ADDRESS _____
☐ Individual ☐ Small Business Concern ☐ Nonprofit Organization

FULL NAME _____
ADDRESS _____
☐ Individual ☐ Small Business Concern ☐ Nonprofit Organization

Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

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, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING: Shlomo Touboul

TITLE OF PERSON SIGNING OTHER THAN OWNER: Chairman of the Board

ADDRESS OF PERSON SIGNING: Kefar-Haim, Israel 42945

SIGNATURE: _____ DATE: 13.5.98

Patent and Trademark Office-U.S. DEPARTMENT OF COMMERCE