PTO/AIA/15 (03-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	FIN0009-CIP1-CON1
First Named Inventor	Yuval Ben-Itzhak, et al.
Title	Computer Security Method and System With Input Parameter Validation
Express Mail Label No.	

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☐ **Fee Transmittal Form** (PTO/SB/17 or equivalent)
2. ☐ **Applicant asserts small entity status.** See 37 CFR 1.27
3. ☐ **Applicant certifies micro entity status.** See 37 CFR 1.29. Applicant must attach form PTO/SB/15A or B or equivalent.
4. ☑ **Specification** [*Total Pages* 21] Both the claims and abstract must start on a new page. *(See MPEP § 608.01(a) for information on the preferred arrangement)*
5. ☑ **Drawing(s)** (35 U.S.C. 113) [*Total Sheets* 3]
6. **Inventor's Oath or Declaration** [*Total Pages* ____] *(including substitute statements under 37 CFR 1.64 and assignments serving as an oath or declaration under 37 CFR 1.63(e))*
   a. ☐ Newly executed (original or copy)
   b. ☐ A copy from a prior application (37 CFR 1.63(d))
7. ☑ **Application Data Sheet** ** See note below.* See 37 CFR 1.76 (PTO/AIA/14 or equivalent)
8. **CD-ROM or CD-R** in duplicate, large table, or Computer Program (*Appendix*)
   ☐ Landscape Table on CD
9. **Nucleotide and/or Amino Acid Sequence Submission** (*if applicable, items a. – c. are required*)
   a. ☐ Computer Readable Form (CRF)
   b. ☐ Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statements verifying identity of above copies

ADDRESS TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**

ACCOMPANYING APPLICATION PAPERS

10. ☐ **Assignment Papers** (cover sheet & document(s)) Name of Assignee ____
11. ☐ **37 CFR 3.73(c) Statement** (*when there is an assignee*) ☐ **Power of Attorney**
12. ☐ **English Translation Document** (*if applicable*)
13. ☑ **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
    ☐ Copies of citations attached
14. ☐ **Preliminary Amendment**
15. ☐ **Return Receipt Postcard** (*MPEP § 503*) (*Should be specifically itemized*)
16. ☐ **Certified Copy of Priority Document(s)** (*if foreign priority is claimed*)
17. ☐ **Nonpublication Request** Under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
18. ☑ **Other:** Certification and Request for Prioritized Examination Under 37 C.F.R. 1.102(e). Filed Electronically.

***Note**: (1) Benefit claims under 37 CFR 1.78 and foreign priority claims under 1.55 **must** be included in an Application Data Sheet (ADS).
(2) For applications filed under 35 U.S.C. 111, the application must contain an ADS specifying the applicant if the applicant is an assignee, person to whom the inventor is under an obligation to assign, or person who otherwise shows sufficient proprietary interest in the matter. See 37 CFR 1.46(b).

19. CORRESPONDENCE ADDRESS

☑ The address associated with Customer Number: 115222 **OR** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature	/Dawn-Marie Bey/	Date	September 10, 2014
Name (Print/Type)	Dawn-Marie Bey	Registration No. (Attorney/Agent)	44,442

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.

COMPUTER SECURITY METHOD AND SYSTEM WITH INPUT PARAMETER VALIDATION

PRIORITY REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of pending U.S. Patent Application No. 12/174,592, filed on July 16, 2008, entitled "COMPUTER SECURITY METHOD AND SYSTEM WITH INPUT PARAMETER VALIDATION," which is a continuation-in-part of U.S. Patent Application No. 11/354,893, filed on February 16, 2006, entitled SYSTEM AND METHOD FOR ENFORCING A SECURITY CONTEXT ON A DOWNLOADABLE, now U.S. Patent No. 7,613,918, and is a continuation-in-part of U.S. Patent Application No. 11/298,475, filed December 12, 2005, entitled "SYSTEM AND METHOD FOR INSPECTING DYNAMICALLY GENERATED EXECUTABLE CODE," now U.S. Patent No. 7,757,289.

FIELD OF THE INVENTION

[0002] The field of the present invention is computer security.

BACKGROUND OF THE INVENTION

[0003] Computer security software and hardware are used to inspect downloadables, to determine if they are malicious. The term "downloadable" refers generally to an executable application program, which is downloaded from a source computer and run on a destination computer. There are many different types of malicious downloadables, including malware, phishing, spyware, Trojan horses, viruses and worms. Malicious downloadables often enter an internal computer network from an external network, and infect all or most of the computers in the internal network once they break in. As such, computer security systems often employ gateway computers to scan and filter incoming downloadables.

[0004] Scanning downloadables at a gateway computer may be performed by running the programs; however, running the programs on the gateway computer instead of on the computer in the internal network for which the programs are intended, may result in the gateway computer failing to detect exploits in the downloadables.

[0005] Scanning downloadables at a gateway computer may also be performed by analyzing the programs. Assignee's U.S. Patent No. 6,092,194 describes such a gateway security system.

[0006] When analyzing downloadables, scanners generally search for computer operations that are potentially suspicious. For example, if a suspect downloadable invokes a function call that writes to a file system or opens a network connection or changes a registry entry, such behavior raises a warning flag for potentially malicious activity. A security system may block a downloadable from reaching an internal network if the downloadable includes a suspicious computer operation. However, most non-malicious downloadables use these same computer operations in an innocuous way, and such a security system may block both good and bad downloadables from reaching the internal network.

[0007] Consider, for example, a function that deletes a file in the file system. Many safe programs, such as software installation programs, generate temporary files during execution, and delete the temporary files upon completion. However, a malicious program may delete critical operating system files. A security system that blocks downloadables which invoke a function to delete a file would block safe downloadables in addition to the malicious ones.

[0008] Consider, for example, a downloadable that includes the following simple JavaScript source code:

```
<SCRIPT LANGUAGE="JavaScript">
        var b = new ActiveXObject("Msxml2.XMLHTTP");
        exploit data = "SSSSSSSSSSSSSSSSSSSSSS  exploit";
```

```
        b.setRequestHeader(exploit data);
</SCRIPT>
```

This source code initiates a new Msxml2.XMLHTTP ActiveX object, and invokes the object's method setRequestHeader(). An Msxml2.XMLHTTP object is a standard object built into the Microsoft XML parser. The Msxml2.XMLHTTP object is an important part of the Ajax web development technique, and is used to implement responsive and dynamic web applications. It is used on a client side web page to grab information from the server, process it, and use the information on the current web page (as opposed to having to reload a web page).

[0009] The method setRequestHeader() is generally a safe function that simply adds an HTTP header to a request. The following code snippet shows how setRequestHeader() is used, for example, to set the HTTP Content-Type header to 'text/xml' before sending a request body.

```
var oReq = new XMLHttpRequest();
oReq.open("POST", sURL, false);
oReq.setRequestHeader(CONTENT, "text/xml");
oReq.send(sRequestBody);
```

As such, the example JavaScript above appears innocuous.

[0010] However, the input parameter to setRequestHeader() in the example JavaScript code above is only evaluated at run-time, and a code exploit may be triggered in the process of evaluating the input parameter. More generally, input parameters to function calls, even for safe functions, are potential hiding places for code exploits. Since input parameters may only be determined at run-time, such code exploits may go undetected when scanning downloadables.

[0011] It would thus be of advantage for a security system to be able to validate input parameters that are evaluated at run-time. It would be of further advantage for a security system to be able to determine if a given input parameter will exploit a non-malicious function, prior to actually executing the non-malicious function with the given input

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.