

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants : Yigal Mordechai Edery et al.
U.S. Serial No. : unknown
Filed : herewith
Title : MALICIOUS MOBILE CODE RUNTIME MONITORING
SYSTEM AND METHODS
Group Art Unit : unknown
Examiner : unknown

EXPRESS MAIL MAILING LABEL NUMBER EQ 399946563 US, Date of Deposit: March 7, 2006

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Andrew L. Tiajolloff
(Name of person mailing paper or fee)

(Signature of person mailing paper or fee)

March 7, 2006
Date

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PATENT APPLICATION TRANSMITTAL LETTER

Sir:

Attorney for the above-captioned applicants transmits herewith the following:

1. a fee transmittal sheet (1 page);
2. an application data sheet (3 pages);
3. the application, which is a copy of the parent application as filed, comprising a cover sheet (1 page), specification (42 pages), claims (15 pages), drawings (10 pages), and abstract (1 page);

ELG-P-9139US2

4. a copy of an executed declaration of the inventors from the parent application;
- and
5. a Preliminary Amendment and Information Disclosure Statement.

PLEASE ASSOCIATE THIS APPLICATION WITH CUSTOMER NUMBER

43214.

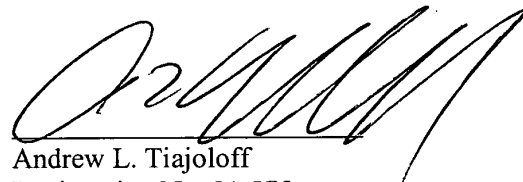
Should any questions arise, the Patent Office is invited to telephone attorney for applicants at 212-490-3285.

CUSTOMER NUMBER
43214
U.S. PATENT TRADEMARK OFFICE

Tiajolloff & Kelly
Chrysler Building, 37th floor
405 Lexington Avenue
New York, NY 10174

tel. 212-490-3285
fax 212-490-3295

Respectfully submitted,



Andrew L. Tiajolloff
Registration No. 31,575

030706

20427 U.S. PTO

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 2005

Effective 12/08/2004

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT (\$7350)

Complete if Known

Application Number	
Filing Date	
First Named Inventor	EDERY, Yigal Mordechai
Examiner Name	
Group / Art Unit	
Attorney Docket No.	P-9139-US2

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please specify): _____

☒ Deposit Account Number 50-3400

Deposit Account Name: Eitan Law Group

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below

☐ Charge fee(s) indicated below, except for the filing fee

☒ Charge any additional fee(s) or underpayments of fee(s)
 under 37 CFE 1.16 and 1.17

☒ Credit any overpayments

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.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES		SEARCH FEES		EXAMINATION FEES		Fees Paid (\$)
	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	
Utility	300	150	500	250	200	100	1000
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee (\$)	Small Entity Fee (\$)
Each claim over 20 or, for Reissues, each claim over 20 and more than in the original patent	50	25
Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent	200	100
Multiple dependent claims	360	180
Total Claims		
75 -20 or HP = 55	50	2750
HP = highest number of total claims paid for, if greater than 20.		
Indep. Claims		
21 -3 or HP = 18	200	3600
HP = highest number of independent claims paid for, if greater than 3.		

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee (\$)	Fee Paid (\$)
100	0	0	0	0

4. OTHER FEE(S)

Non-English Specification, \$130 fee (no small entity discount)

Other fee(s):

SUBMITTED BY		Complete (if applicable)	
Name (Print /Type)	Tally Eitan	Registration No. (Attorney/Agent)	Telephone (212) 490-3285
Signature		Date	March 7, 2006

This collection of information is required by 37 CFR 1.136. 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 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants : Yigal Mordechai Edery et al.
U.S. Serial No. : unknown
Filed : herewith
Title : MALICIOUS MOBILE CODE RUNTIME MONITORING
SYSTEM AND METHODS
Group Art Unit : unknown
Examiner : unknown

EXPRESS MAIL MAILING LABEL NUMBER EQ 399946563 US, Date of Deposit: March 7, 2006

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Andrew L. Tiajolloff
(Name of person mailing paper or fee)

(Signature of person mailing paper or fee)

March 7, 2006
Date

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PATENT APPLICATION TRANSMITTAL LETTER

Sir:

Attorney for the above-captioned applicants transmits herewith the following:

1. a fee transmittal sheet (1 page);
2. an application data sheet (3 pages);
3. the application, which is a copy of the parent application as filed, comprising a cover sheet (1 page), specification (42 pages), claims (15 pages), drawings (10 pages), and abstract (1 page);

ELG-P-9139US2

4. a copy of an executed declaration of the inventors from the parent application;
- and
5. a Preliminary Amendment and Information Disclosure Statement.

PLEASE ASSOCIATE THIS APPLICATION WITH CUSTOMER NUMBER

43214.

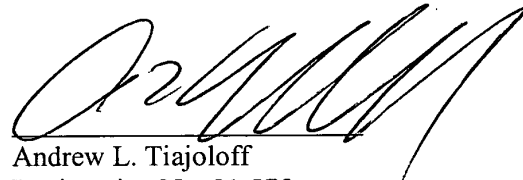
Should any questions arise, the Patent Office is invited to telephone attorney for applicants at 212-490-3285.

CUSTOMER NUMBER
43214
U.S. PATENT TRADEMARK OFFICE

Tiajolloff & Kelly
Chrysler Building, 37th floor
405 Lexington Avenue
New York, NY 10174

tel. 212-490-3285
fax 212-490-3295

Respectfully submitted,



Andrew L. Tiajolloff
Registration No. 31,575

030706

20427 U.S. PTO

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 2005**

Effective 12/08/2004

☐ Applicant claims small entity status. See 37 CFR 1.27**TOTAL AMOUNT OF PAYMENT (\$)** 7350**Complete if Known**

Application Number	
Filing Date	
First Named Inventor	EDERY, Yigal Mordechai
Examiner Name	
Group / Art Unit	
Attorney Docket No.	P-9139-US2

METHOD OF PAYMENT (check all that apply)☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please specify): _____☒ Deposit Account Number **50-3400**Deposit Account Name: **Eitan Law Group**

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below☐ Charge fee(s) indicated below, except for the filing fee☒ Charge any additional fee(s) or underpayments of fee(s)☒ Credit any overpayments**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.**FEE CALCULATION****1. BASIC FILING, SEARCH, AND EXAMINATION FEES**

Application Type	FILING FEES		SEARCH FEES		EXAMINATION FEES		Fees Paid (\$)
	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	
Utility	300	150	500	250	200	100	1000
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee (\$)	Small Entity Fee (\$)
Each claim over 20 or, for Reissues, each claim over 20 and more than in the original patent	50	25
Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent	200	100
Multiple dependent claims	360	180
Total Claims		
75 -20 or HP = 55	50	2750
HP = highest number of total claims paid for, if greater than 20.		
Indep. Claims		
21 -3 or HP = 18	200	3600
HP = highest number of independent claims paid for, if greater than 3.		

3. APPLICATION SIZE FEE

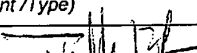
If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee (\$)	Fee Paid (\$)
100	0	0	0	0

4. OTHER FEE(S)

Non-English Specification, \$130 fee (no small entity discount)

Other fee(s): _____

SUBMITTED BY		Complete (if applicable)	
Name (Print /Type)	Tally Eitan	Registration No. (Attorney/Agent)	Telephone (212) 490-3285
Signature		Date	March 7, 2006

This collection of information is required by 37 CFR 1.136. 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 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

**APPLICATION FOR
UNITED STATES PATENT
IN THE NAME OF**

Yigal Edery, Nimrod Vered and David Kroll

OF

FINJAN SOFTWARE, LTD.

**MALICIOUS MOBILE CODE RUNTIME MONITORING
SYSTEM AND METHODS**

DOCKET NO. 43426.00014

Please direct communications to:

**Intellectual Property Department
Squire, Sanders & Dempsey L.L.P.
600 Hansen Way
Palo Alto, CA 94304-1043
(650) 856-6500**

Express Mail Number EL 701 364 624

MALICIOUS MOBILE CODE RUNTIME MONITORING

SYSTEM AND METHODS

PRIORITY REFERENCE TO RELATED APPLICATIONS

5 This application claims benefit of and hereby incorporates by reference
provisional application serial number 60/205,591, entitled "Computer Network Malicious
Code Run-time Monitoring," filed on May 17, 2000 by inventors Nimrod Itzhak Vered, et
al. This application is also a Continuation-In-Part of and hereby incorporates by
reference patent application serial number 09/539,667, entitled "System and Method for
10 Protecting a Computer and a Network From Hostile Downloadables" filed on March 30,
2000 by inventor Shlomo Touboul. This application is also a Continuation-In-Part of and
hereby incorporates by reference patent application serial number 09/551,302, entitled
"System and Method for Protecting a Client During Runtime From Hostile
Downloadables", filed on April 18, 2000 by inventor Shlomo Touboul.

BACKGROUND OF THE INVENTION

Field of the Invention

20 This invention relates generally to computer networks, and more particularly
provides a system and methods for protecting network-connectable devices from
undesirable downloadable operation.

Description of the Background Art

Advances in networking technology continue to impact an increasing number and diversity of users. The Internet, for example, already provides to expert, intermediate and even novice users the informational, product and service resources of over 100,000 interconnected networks owned by governments, universities, nonprofit groups, companies, etc. Unfortunately, particularly the Internet and other public networks have also become a major source of potentially system-fatal or otherwise damaging computer code commonly referred to as "viruses."

Efforts to forestall viruses from attacking networked computers have thus far met with only limited success at best. Typically, a virus protection program designed to identify and remove or protect against the initiating of known viruses is installed on a network firewall or individually networked computer. The program is then inevitably surmounted by some new virus that often causes damage to one or more computers. The damage is then assessed and, if isolated, the new virus is analyzed. A corresponding new virus protection program (or update thereof) is then developed and installed to combat the new virus, and the new program operates successfully until yet another new virus appears - and so on. Of course, damage has already typically been incurred.

To make matters worse, certain classes of viruses are not well recognized or understood, let alone protected against. It is observed by this inventor, for example, that Downloadable information comprising program code can include distributable components (e.g. Java™ applets and JavaScript scripts, ActiveX™ controls, Visual Basic, add-ins and/or others). It can also include, for example, application programs, Trojan horses, multiple compressed programs such as zip or meta files, among others. U.S. Patent 5,983,348 to Shuang, however, teaches a protection system for protecting

against only distributable components including “Java applets or ActiveX controls”, and further does so using resource intensive and high bandwidth static Downloadable content and operational analysis, and modification of the Downloadable component; Shuang further fails to detect or protect against additional program code included within a tested

5 Downloadable. U.S. Patent 5,974,549 to Golan teaches a protection system that further focuses only on protecting against ActiveX controls and not other distributable components, let alone other Downloadable types. U.S. patent 6,167,520 to Touboul enables more accurate protection than Shuang or Golan, but lacks the greater flexibility and efficiency taught herein, as do Shuang and Golan.

10 Accordingly, there remains a need for efficient, accurate and flexible protection of computers and other network connectable devices from malicious Downloadables.

SUMMARY OF THE INVENTION

15 The present invention provides protection systems and methods capable of protecting a personal computer (“PC”) or other persistently or even intermittently network accessible devices or processes from harmful, undesirable, suspicious or other “malicious” operations that might otherwise be effectuated by remotely operable code. While enabling the capabilities of prior systems, the present invention is not nearly so limited, resource intensive or inflexible, and yet enables more reliable protection. For

20 example, remotely operable code that is protectable against can include downloadable application programs, Trojan horses and program code groupings, as well as software “components”, such as Java™ applets, ActiveX™ controls, JavaScript™/Visual Basic scripts, add-ins, etc., among others. Protection can also be provided in a distributed

interactively, automatically or mixed configurable manner using protected client, server or other parameters, redirection, local/remote logging, etc., and other server/client based protection measures can also be separately and/or interoperably utilized, among other examples.

5 In one aspect, embodiments of the invention provide for determining, within one or more network “servers” (e.g. firewalls, resources, gateways, email relays or other devices/processes that are capable of receiving-and-transferring a Downloadable) whether received information includes executable code (and is a “Downloadable”). Embodiments also provide for delivering static, configurable and/or extensible remotely operable protection policies to a Downloadable-destination, more typically as a sandboxed package including the mobile protection code, downloadable policies and one or more received Downloadables. Further client-based or remote protection code/policies can also be utilized in a distributed manner. Embodiments also provide for causing the mobile protection code to be executed within a Downloadable-destination in a manner that enables various Downloadable operations to be detected, intercepted or further responded to via protection operations. Additional server/information-destination device security or other protection is also enabled, among still further aspects.

A protection engine according to an embodiment of the invention is operable within one or more network servers, firewalls or other network connectable information re-communicating devices (as are referred to herein summarily one or more “servers” or “re-communicators”). The protection engine includes an information monitor for monitoring information received by the server, and a code detection engine for determining whether the received information includes executable code. The protection

engine also includes a packaging engine for causing a sandboxed package, typically including mobile protection code and downloadable protection policies to be sent to a Downloadable-destination in conjunction with the received information, if the received information is determined to be a Downloadable.

5 A sandboxed package according to an embodiment of the invention is receivable by and operable with a remote Downloadable-destination. The sandboxed package includes mobile protection code ("MPC") for causing one or more predetermined malicious operations or operation combinations of a Downloadable to be monitored or otherwise intercepted. The sandboxed package also includes protection policies (operable
10 alone or in conjunction with further Downloadable-destination stored or received policies/MPCs) for causing one or more predetermined operations to be performed if one or more undesirable operations of the Downloadable is/are intercepted. The sandboxed package can also include a corresponding Downloadable and can provide for initiating the Downloadable in a protective "sandbox". The MPC/policies can further include a
15 communicator for enabling further MPC/policy information or "modules" to be utilized and/or for event logging or other purposes.

A sandbox protection system according to an embodiment of the invention comprises an installer for enabling a received MPC to be executed within a Downloadable-destination (device/process) and further causing a Downloadable
20 application program, distributable component or other received downloadable code to be received and installed within the Downloadable-destination. The protection system also includes a diverter for monitoring one or more operation attempts of the Downloadable, an operation analyzer for determining one or more responses to the attempts, and a

security enforcer for effectuating responses to the monitored operations. The protection system can further include one or more security policies according to which one or more protection system elements are operable automatically (e.g. programmatically) or in conjunction with user intervention (e.g. as enabled by the security enforcer). The security policies can also be configurable/extensible in accordance with further downloadable and/or Downloadable-destination information.

A method according to an embodiment of the invention includes receiving downloadable information, determining whether the downloadable information includes executable code, and causing a mobile protection code and security policies to be communicated to a network client in conjunction with security policies and the downloadable information if the downloadable information is determined to include executable code. The determining can further provide multiple tests for detecting, alone or together, whether the downloadable information includes executable code.

A further method according to an embodiment of the invention includes forming a sandboxed package that includes mobile protection code ("MPC"), protection policies, and a received, detected-Downloadable, and causing the sandboxed package to be communicated to and installed by a receiving device or process ("user device") for responding to one or more malicious operation attempts by the detected-Downloadable from within the user device. The MPC/policies can further include a base "module" and a "communicator" for enabling further up/downloading of one or more further "modules" or other information (e.g. events, user/user device information, etc.).

Another method according to an embodiment of the invention includes installing, within a user device, received mobile protection code ("MPC") and protection policies in

conjunction with the user device receiving a downloadable application program, component or other Downloadable(s). The method also includes determining, by the MPC, a resource access attempt by the Downloadable, and initiating, by the MPC, one or more predetermined operations corresponding to the attempt. (Predetermined operations can, for example, comprise initiating user, administrator, client, network or protection system determinable operations, including but not limited to modifying the Downloadable operation, extricating the Downloadable, notifying a user/another, maintaining a local/remote log, causing one or more MPCs/policies to be downloaded, etc.)

Advantageously, systems and methods according to embodiments of the invention enable potentially damaging, undesirable or otherwise malicious operations by even unknown mobile code to be detected, prevented, modified and/or otherwise protected against without modifying the mobile code. Such protection is further enabled in a manner that is capable of minimizing server and client resource requirements, does not require pre-installation of security code within a Downloadable-destination, and provides for client specific or generic and readily updateable security measures to be flexibly and efficiently implemented. Embodiments further provide for thwarting efforts to bypass security measures (e.g. by "hiding" undesirable operation causing information within apparently inert or otherwise "friendly" downloadable information) and/or dividing or combining security measures for even greater flexibility and/or efficiency.

Embodiments also provide for determining protection policies that can be downloaded and/or ascertained from other security information (e.g. browser settings, administrative policies, user input, uploaded information, etc.). Different actions in response to different Downloadable operations, clients, users and/or other criteria are also

enabled, and embodiments provide for implementing other security measures, such as verifying a downloadable source, certification, authentication, etc. Appropriate action can also be accomplished automatically (e.g. programmatically) and/or in conjunction with alerting one or more users/administrators, utilizing user input, etc. Embodiments

5 further enable desirable Downloadable operations to remain substantially unaffected, among other aspects.

006139 051701
FOI 90 621980
10
15

BRIEF DESCRIPTION OF THE DRAWINGS

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

FIG. 1b is a block diagram illustrating a network subsystem example in
5 accordance with an embodiment of the invention;

FIG. 1c is a block diagram illustrating a further network subsystem example in accordance with an embodiment of the invention;

FIG. 2 is a block diagram illustrating a computer system in accordance with an embodiment of the invention;

10 FIG. 3 is a flow diagram broadly illustrating a protection system host according to an embodiment of the invention;

FIG. 4 is a block diagram illustrating a protection engine according to an embodiment of the invention;

15 FIG. 5 is a block diagram illustrating a content inspection engine according to an embodiment of the invention;

FIG. 6a is a block diagram illustrating protection engine parameters according to an embodiment of the invention;

FIG. 6b is a flow diagram illustrating a linking engine use in conjunction with ordinary, compressed and distributable sandbox package utilization, according to an
20 embodiment of the invention;

FIG. 7a is a flow diagram illustrating a sandbox protection system operating within a destination system, according to an embodiment of the invention;

FIG. 7b is a block diagram illustrating memory allocation usable in conjunction with the protection system of FIG. 7a, according to an embodiment of the invention;

FIG. 7c is a block diagram illustrating a mobile protection code according to an embodiment of the invention;

5 FIG. 8 is a flowchart illustrating a method for examining a Downloadable in accordance with the present invention;

FIG. 9 is a flowchart illustrating a server based protection method according to an embodiment of the invention;

10 FIG. 10a is a flowchart illustrating method for determining if a potential-Downloadable includes or is likely to include executable code, according to an embodiment of the invention;

FIG. 10b is a flowchart illustrating a method for forming a protection agent, according to an embodiment of the invention;

15 FIG. 11 is a flowchart illustrating a method for protecting a Downloadable destination according to an embodiment of the invention;

FIG. 12a is a flowchart illustrating a method for forming a Downloadable access interceptor according to an embodiment of the invention; and

FIG. 12b is a flowchart illustrating a method for implementing mobile protection policies according to an embodiment of the invention.

20

DETAILED DESCRIPTION

In providing malicious mobile code runtime monitoring systems and methods, embodiments of the invention enable actually or potentially undesirable operations of even unknown malicious code to be efficiently and flexibly avoided. Embodiments
5 provide, within one or more “servers” (e.g. firewalls, resources, gateways, email relays or other information re-communicating devices), for receiving downloadable-information and detecting whether the downloadable-information includes one or more instances of executable code (e.g. as with a Trojan horse, zip/meta file etc.). Embodiments also provide for separately or interoperably conducting additional security measures within the
10 server, within a Downloadable-destination of a detected-Downloadable, or both.

Embodiments further provide for causing mobile protection code (“MPC”) and downloadable protection policies to be communicated to, installed and executed within one or more received information destinations in conjunction with a detected-Downloadable. Embodiments also provide, within an information-destination, for
15 detecting malicious operations of the detected-Downloadable and causing responses thereto in accordance with the protection policies (which can correspond to one or more user, Downloadable, source, destination, or other parameters), or further downloaded or downloadable-destination based policies (which can also be configurable or extensible). (Note that the term “or”, as used herein, is generally intended to mean “and/or” unless
20 otherwise indicated.)

FIGS. 1a through 1c illustrate a computer network system 100 according to an embodiment of the invention. FIG. 1a broadly illustrates system 100, while FIGS. 1b and

1c illustrate exemplary protectable subsystem implementations corresponding with system 104 or 106 of FIG. 1a.

Beginning with FIG. 1a, computer network system 100 includes an external computer network 101, such as a Wide Area Network or “WAN” (e.g. the Internet), which is coupled to one or more network resource servers (summarily depicted as resource server-1 102 and resource server-N 103). Where external network 101 includes the Internet, resource servers 1-N (102, 103) might provide one or more resources including web pages, streaming media, transaction-facilitating information, program updates or other downloadable information, summarily depicted as resources 121, 131 and 132. Such information can also include more traditionally viewed “Downloadables” or “mobile code” (i.e. distributable components), as well as downloadable application programs or other further Downloadables, such as those that are discussed herein. (It will be appreciated that interconnected networks can also provide various other resources as well.)

Also coupled via external network 101 are subsystems 104-106. Subsystems 104-106 can, for example, include one or more servers, personal computers (“PCs”), smart appliances, personal information managers or other devices/processes that are at least temporarily or otherwise intermittently directly or indirectly connectable in a wired or wireless manner to external network 101 (e.g. using a dialup, DSL, cable modem, cellular connection, IR/RF, or various other suitable current or future connection alternatives). One or more of subsystems 104-106 might further operate as user devices that are connectable to external network 101 via an internet service provider (“ISP”) or

local area network ("LAN"), such as a corporate intranet, or home, portable device or smart appliance network, among other examples.

FIG. 1a also broadly illustrates how embodiments of the invention are capable of selectively, modifiably or extensibly providing protection to one or more determinable
 5 ones of networked subsystems 104-106 or elements thereof (not shown) against potentially harmful or other undesirable ("malicious") effects in conjunction with receiving downloadable information. "Protected" subsystem 104, for example, utilizes a protection in accordance with the teachings herein, while "unprotected" subsystem-N 105
 10 employs no protection, and protected subsystem-M 106 might employ one or more protections including those according to the teachings herein, other protection, or some combination.

System 100 implementations are also capable of providing protection to redundant elements 107 of one or more of subsystems 104-106 that might be utilized, such as backups, failsafe elements, redundant networks, etc. Where included, such redundant
 15 elements are also similarly protectable in a separate, combined or coordinated manner using embodiments of the present invention either alone or in conjunction with other protection mechanisms. In such cases, protection can be similarly provided singly, as a composite of component operations or in a backup fashion. Care should, however, be exercised to avoid potential repeated protection engine execution corresponding to a
 20 single Downloadable; such "chaining" can cause a Downloadable to operate incorrectly or not at all, unless a subsequent detection engine is configured to recognize a prior packaging of the Downloadable..

FIGS. 1b and 1c further illustrate, by way of example, how protection systems according to embodiments of the invention can be utilized in conjunction with a wide variety of different system implementations. In the illustrated examples, system elements are generally configurable in a manner commonly referred to as a “client-server” configuration, as is typically utilized for accessing Internet and many other network resources. For clarity sake, a simple client-server configuration will be presumed unless otherwise indicated. It will be appreciated, however, that other configurations of interconnected elements might also be utilized (e.g. peer-peer, routers, proxy servers, networks, converters, gateways, services, network reconfiguring elements, etc.) in accordance with a particular application.

The FIG. 1b example shows how a suitable protected system 104a (which can correspond to subsystem-1 104 or subsystem-M 106 of FIG. 1) can include a protection-initiating host “server” or “re-communicator” (e.g. ISP server 140a), one or more user devices or “Downloadable-destinations” 145, and zero or more redundant elements (which elements are summarily depicted as redundant client device/process 145a). In this example, ISP server 140a includes one or more email, Internet or other servers 141a, or other devices or processes capable of transferring or otherwise “re-communicating” downloadable information to user devices 145. Server 141a further includes protection engine or “PE” 142a, which is capable of supplying mobile protection code (“MPC”) and protection policies for execution by client devices 145. One or more of user devices 145 can further include a respective one or more clients 146 for utilizing information received via server 140a, in accordance with which MPC and protection policies are operable to

protect user devices 145 from detrimental, undesirable or otherwise “malicious” operations of downloadable information also received by user device 145.

The FIG. 1c example shows how a further suitable protected system 104b can include, in addition to a “re-communicator”, such as server 142b, a firewall 143c (e.g. as is typically the case with a corporate intranet and many existing or proposed home/smart networks.) In such cases, a server 141b or firewall 143 can operate as a suitable protection engine host. A protection engine can also be implemented in a more distributed manner among two or more protection engine host systems or host system elements, such as both of server 141b and firewall 143, or in a more integrated manner, for example, as a standalone device. Redundant system or system protection elements can also be similarly provided in a more distributed or integrated manner (see above).

00361330-054704
10
15

System 104b also includes internal network 144 and user devices 145. User devices 145 further include a respective one or more clients 146 for utilizing information received via server 140a, in accordance with which the MPCs or protection policies are operable. (As in the previous example, one or more of user devices 145 can also include or correspond with similarly protectable redundant system elements, which are not shown.)

It will be appreciated that the configurations of FIGS 1a-1c are merely exemplary. Alternative embodiments might, for example, utilize other suitable connections, devices or processes. One or more devices can also be configurable to operate as a network server, firewall, smart router, a resource server servicing deliverable third-party/manufacture postings, a user device operating as a firewall/server, or other information-suppliers or intermediaries (i.e. as a “re-communicator” or “server”) for

servicing one or more further interconnected devices or processes or interconnected levels of devices or processes. Thus, for example, a suitable protection engine host can include one or more devices or processes capable of providing or supporting the providing of mobile protection code or other protection consistent with the teachings herein. A suitable information-destination or “user device” can further include one or more devices or processes (such as email, browser or other clients) that are capable of receiving and initiating or otherwise hosting a mobile code execution.

FIG. 2 illustrates an exemplary computing system 200, that can comprise one or more of the elements of FIGS. 1a through 1c. While other application-specific alternatives might be utilized, it will be presumed for clarity sake that system 100 elements (FIGS. 1a-c) are implemented in hardware, software or some combination by one or more processing systems consistent therewith, unless otherwise indicated.

Computer system 200 comprises elements coupled via communication channels (e.g. bus 201) including one or more general or special purpose processors 202, such as a Pentium® or Power PC®, digital signal processor (“DSP”), etc. System 200 elements also include one or more input devices 203 (such as a mouse, keyboard, microphone, pen, etc.), and one or more output devices 204, such as a suitable display, speakers, actuators, etc., in accordance with a particular application.

System 200 also includes a computer readable storage media reader 205 coupled to a computer readable storage medium 206, such as a storage/memory device or hard or removable storage/memory media; such devices or media are further indicated separately as storage device 208 and memory 209, which can include hard disk variants, floppy/compact disk variants, digital versatile disk (“DVD”) variants, smart cards, read

only memory, random access memory, cache memory, etc., in accordance with a particular application. One or more suitable communication devices 207 can also be included, such as a modem, DSL, infrared or other suitable transceiver, etc. for providing inter-device communication directly or via one or more suitable private or public

5 networks that can include but are not limited to those already discussed.

Working memory further includes operating system ("OS") elements and other programs, such as application programs, mobile code, data, etc. for implementing system 100 elements that might be stored or loaded therein during use. The particular OS can vary in accordance with a particular device, features or other aspects in accordance with a particular application (e.g. Windows, Mac, Linux, Unix or Palm OS variants, a

10 proprietary OS, etc.). Various programming languages or other tools can also be utilized, such as C++, Java, Visual Basic, etc. As will be discussed, embodiments can also include a network client such as a browser or email client, e.g. as produced by Netscape, Microsoft or others, a mobile code executor such as an OS task manager, Java Virtual

15 Machine ("JVM"), etc., and an application program interface ("API"), such as a Microsoft Windows or other suitable element in accordance with the teachings herein. (It will also become apparent that embodiments might also be implemented in conjunction with a resident application or combination of mobile code and resident application components.)

20 One or more system 200 elements can also be implemented in hardware, software or a suitable combination. When implemented in software (e.g. as an application program, object, downloadable, servlet, etc. in whole or part), a system 200 element can be communicated transitionally or more persistently from local or remote storage to

memory (or cache memory, etc.) for execution, or another suitable mechanism can be utilized, and elements can be implemented in compiled or interpretive form. Input, intermediate or resulting data or functional elements can further reside more transitionally or more persistently in a storage media, cache or more persistent volatile or non-volatile memory, (e.g. storage device 207 or memory 208) in accordance with a particular application.

FIG. 3 illustrates an interconnected re-communicator 300 generally consistent with system 140b of FIG. 1, according to an embodiment of the invention. As with system 140b, system 300 includes a server 301, and can also include a firewall 302. In this implementation, however, either server 301 or firewall 302 (if a firewall is used) can further include a protection engine (310 or 320 respectively). Thus, for example, an included firewall can process received information in a conventional manner, the results of which can be further processed by protection engine 310 of server 301, or information processed by protection engine 320 of an included firewall 302 can be processed in a conventional manner by server 301. (For clarity sake, a server including a singular protection engine will be presumed, with or without a firewall, for the remainder of the discussion unless otherwise indicated. Note, however, that other embodiments consistent with the teachings herein might also be utilized.)

FIG. 3 also shows how information received by server 301 (or firewall 302) can include non-executable information, executable information or a combination of non-executable and one or more executable code portions (e.g. so-called Trojan horses that include a hostile Downloadable within a friendly one, combined, compressed or otherwise encoded files, etc.). Particularly such combinations will likely remain

undetected by a firewall or other more conventional protection systems. Thus, for convenience, received information will also be referred to as a “potential-Downloadable”, and received information found to include executable code will be referred to as a “Downloadable” or equivalently as a “detected-Downloadable” (regardless of whether the executable code includes one or more application programs, distributable “components” such as Java, ActiveX, add-in, etc.).

Protection engine 310 provides for detecting whether received potential-Downloadables include executable code, and upon such detection, for causing mobile protection code (“MPC”) to be transferred to a device that is a destination of the potential-Downloadable (or “Downloadable-destination”). Protection engine 310 can also provide protection policies in conjunction with the MPC (or thereafter as well), which MPC/policies can be automatically (e.g. programmatically) or interactively configurable in accordance user, administrator, downloadable source, destination, operation, type or various other parameters alone or in combination (see below). Protection engine 310 can also provide or operate separately or interoperably in conjunction with one or more of certification, authentication, downloadable tagging, source checking, verification, logging, diverting or other protection services via the MPC, policies, other local/remote server or destination processing, etc. (e.g. which can also include protection mechanisms taught by the above-noted prior applications; see FIG. 4).

Operationally, protection engine 310 of server 301 monitors information received by server 301 and determines whether the received information is deliverable to a protected destination, e.g. using a suitable monitor/data transfer mechanism and comparing a destination-address of the received information to a protected destination set,

such as a protected destinations list, array, database, etc. (All deliverable information or one or more subsets thereof might also be monitored.) Protection engine 310 further analyzes the potential-Downloadable and determines whether the potential-Downloadable includes executable code. If not, protection engine 310 enables the not executable

5 potential-Downloadable 331 to be delivered to its destination in an unaffected manner.

In conjunction with determining that the potential-Downloadable is a detected-Downloadable, protection engine 310 also causes mobile protection code or "MPC" 341 to be communicated to the Downloadable-destination of the Downloadable, more suitably in conjunction with the detected-Downloadable 343 (see below). Protection engine 310

10 further causes downloadable protection policies 342 to be delivered to the Downloadable-destination, again more suitably in conjunction with the detected-Downloadable. Protection policies 342 provide parameters (or can additionally or alternatively provide additional mobile code) according to which the MPC is capable of determining or providing applicable protection to a Downloadable-destination against malicious

15 Downloadable operations.

(One or more "checked", tag, source, destination, type, detection or other security result indicators, which are not shown, can also be provided as corresponding to determined non-Downloadables or Downloadables, e.g. for testing, logging, further processing, further identification tagging or other purposes in accordance with a particular

20 application.)

Further MPCs, protection policies or other information are also deliverable to a the same or another destination, for example, in accordance with communication by an MPC/protection policies already delivered to a downloadable-destination. Initial or

subsequent MPCs/policies can further be selected or configured in accordance with a Downloadable-destination indicated by the detected-Downloadable, destination-user or administrative information, or other information providable to protection engine 310 by a user, administrator, user system, user system examination by a communicated MPC, etc.

- 5 (Thus, for example, an initial MPC/policies can also be initially provided that are operable with or optimized for more efficient operation with different Downloadable-destinations or destination capabilities.)

10 While integrated protection constraints within the MPC might also be utilized, providing separate protection policies has been found to be more efficient, for example, by enabling more specific protection constraints to be more easily updated in conjunction with detected-Downloadable specifics, post-download improvements, testing, etc. Separate policies can further be more efficiently provided (e.g. selected, modified, instantiated, etc.) with or separately from an MPC, or in accordance with the requirements of a particular user, device, system, administration, later improvement, etc., as might also be provided to protection engine 310 (e.g. via user/MPC uploading, querying, parsing a Downloadable, or other suitable mechanism implemented by one or more servers or Downloadable-destinations).

- 20 (It will also become apparent that performing executable code detection and communicating to a downloadable-Destination an MPC and any applicable policies as separate from a detected-Downloadable is more accurate and far less resource intensive than, for example, performing content and operation scanning, modifying a Downloadable, or providing completely Downloadable-destination based security.)

System 300 enables a single or extensible base-MPC to be provided, in anticipation or upon receipt of a first Downloadable, that is utilized thereafter to provide protection of one or more Downloadable-destinations. It is found, however, that providing an MPC upon each detection of a Downloadable (which is also enabled) can
 5 provide a desirable combination of configurability of the MPC/policies and lessened need for management (e.g. given potentially changing user/destination needs, enabling testing, etc.).

Providing an MPC upon each detection of a Downloadable also facilitates a lessened demand on destination resources, e.g. since information-destination resources
 10 used in executing the MPC/policies can be re-allocated following such use. Such alternatives can also be selectively, modifiably or extensibly provided (or further in accordance with other application-specific factors that might also apply.) Thus, for example, a base-MPC or base-policies might be provided to a user device that is/are extensible via additionally downloadable “modules” upon server 301 detection of a
 15 Downloadable deliverable to the same user device, among other alternatives.

In accordance with a further aspect of the invention, it is found that improved efficiency can also be achieved by causing the MPC to be executed within a Downloadable-destination in conjunction with, and further, prior to initiation of the detected Downloadable. One mechanism that provides for greater compatibility and
 20 efficiency in conjunction with conventional client-based Downloadable execution is for a protection engine to form a sandboxed package 340 including MPC 341, the detected-Downloadable 343 and any policies 342. For example, where the Downloadable is a binary executable to be executed by an operating system, protection engine 310 forms a

protected package by concatenating, within sandboxed package 340, MPC 341 for
 delivery to a Downloadable-destination first, followed by protection policies 342 and
 Downloadable 343. (Concatenation or techniques consistent therewith can also be
 utilized for providing a protecting package corresponding to a Java applet for execution
 5 by a JVM of a Downloadable-destination, or with regard to ActiveX controls, add-ins or
 other distributable components, etc.)

The above concatenation or other suitable processing will result in the following.

Upon receipt of sandboxed package 340 by a compatible browser, email or other
 destination-client and activating of the package by a user or the destination-client, the
 operating system (or a suitable responsively initiated distributed component host) will
 10 attempt to initiate sandboxed package 340 as a single Downloadable. Such processing
 will, however, result in initiating the MPC 341 and -in accordance with further aspects of
 the invention- the MPC will initiate the Downloadable in a protected manner, further in
 accordance with any applicable included or further downloaded protection policies 342.
 15 (While system 300 is also capable of ascertaining protection policies stored at a
 Downloadable-destination, e.g. by poll, query, etc. of available destination information,
 including at least initial policies within a suitable protecting package is found to avoid
 associated security concerns or inefficiencies.)

Turning to FIG. 4, a protection engine 400 generally consistent with protection
 20 engine 310 (or 320) of FIG. 3 is illustrated in accordance with an embodiment of the
 invention. Protection engine 400 comprises information monitor 401, detection engine
 402, and protected packaging engine 403, which further includes agent generator 431,
 storage 404, linking engine 405, and transfer engine 406. Protection engine 400 can also

include a buffer 407, for temporarily storing a received potential-Downloadable, or one or more systems for conducting additional authentication, certification, verification or other security processing (e.g. summarily depicted as security system 408) Protection engine 400 can further provide for selectively re-directing, further directing, logging, etc. of a potential/detected Downloadable or information corresponding thereto in conjunction with detection, other security, etc., in accordance with a particular application.

(Note that FIG. 4, as with other figures included herein, also depicts exemplary signal flow arrows; such arrows are provided to facilitate discussion, and should not be construed as exclusive or otherwise limiting.)

Information monitor 401 monitors potential-Downloadables received by a host server and provides the information via buffer 407 to detection engine 402 or to other system 400 elements. Information monitor 401 can be configured to monitor host server download operations in conjunction with a user or a user-device that has logged-on to the server, or to receive information via a server operation hook, servlet, communication channel or other suitable mechanism.

Information monitor 401 can also provide for transferring, to storage 404 or other protection engine elements, configuration information including, for example, user, MPC, protection policy, interfacing or other configuration information (e.g. see FIG. 6). Such configuration information monitoring can be conducted in accordance with a user/device logging onto or otherwise accessing a host server, via one or more of configuration operations, using an applet to acquire such information from or for a particular user, device or devices, via MPC/policy polling of a user device, or via other suitable mechanisms.

Detection engine 402 includes code detector 421, which receives a potential-Downloadable and determines, more suitably in conjunction with inspection parameters 422, whether the potential-Downloadable includes executable code and is thus a “detected-Downloadable”. (Code detector 421 can also include detection processors for performing file decompression or other “decoding”, or such detection-facilitating processing as decryption, utilization/support of security system 408, etc. in accordance with a particular application.)

Detection engine 402 further transfers a detected-downloadable (“XEQ”) to protected packaging engine 403 along with indicators of such detection, or a determined non-executable (“NXEQ”) to transfer engine 406. (Inspection parameters 422 enable analysis criteria to be readily updated or varied, for example, in accordance with particular source, destination or other potential Downloadable impacting parameters, and are discussed in greater detail with reference to FIG. 5). Detection engine 402 can also provide indicators for delivery of initial and further MPCs/policies, for example, prior to or in conjunction with detecting a Downloadable and further upon receipt of an indicator from an already downloaded MPC/policy. A downloaded MPC/policy can further remain resident at a user device with further modules downloaded upon or even after delivery of a sandboxed package. Such distribution can also be provided in a configurable manner, such that delivery of a complete package or partial packages are automatically or interactively determinable in accordance with user/administrative preferences/policies, among other examples.

Packaging engine 403 provides for generating mobile protection code and protection policies, and for causing delivery thereof (typically with a detected-

Downloadable) to a Downloadable-destination for protecting the Downloadable-destination against malicious operation attempts by the detected Downloadable. In this example, packaging engine 403 includes agent generator 431, storage 404 and linking engine 405.

5 Agent generator 431 includes an MPC generator 432 and a protection policy generator 433 for “generating” an MPC and a protection policy (or set of policies) respectively upon receiving one or more “generate MPC/policy” indicators from detection engine 402, indicating that a potential-Downloadable is a detected-Downloadable. MPC generator 432 and protection policy generator 433 provide for generating MPCs and
10 protection policies respectively in accordance with parameters retrieved from storage 404. Agent generator 431 is further capable of providing multiple MPCs/policies, for example, the same or different MPCs/policies in accordance with protecting ones of multiple executables within a zip file, or for providing initial MPCs/policies and then further MPCs/policies or MPC/policy “modules” as initiated by further indicators such as given
15 above, via an indicator of an already downloaded MPC/policy or via other suitable mechanisms. (It will be appreciated that pre-constructed MPCs/policies or other processing can also be utilized, e.g. via retrieval from storage 404, but with a potential decrease in flexibility.)

MPC generator 432 and protection policy generator 433 are further configurable.

20 Thus, for example, more generic MPCs/policies can be provided to all or a grouping of serviced destination-devices (e.g. in accordance with a similarly configured/administered intranet), or different MPCs/policies that can be configured in accordance with one or more of user, network administration, Downloadable-destination or other parameters (e.g.

see FIG. 6). As will become apparent, a resulting MPC provides an operational interface to a destination device/process. Thus, a high degree of flexibility and efficiency is enabled in providing such an operational interface within different or differently configurable user devices/processes or other constraints.

5 Such configurability further enables particular policies to be utilized in accordance with a particular application (e.g. particular system uses, access limitations, user interaction, treating application programs or Java components from a particular known source one way and unknown source ActiveX components, or other considerations). Agent generator 431 further transfers a resulting MPC and protection
10 policy pair to linking engine 405.

15 Linking engine 405 provides for forming from received component elements (see above) a sandboxed package that can include one or more initial or complete MPCs and applicable protection policies, and a Downloadable, such that the sandboxed package will protect a receiving Downloadable-destination from malicious operation by the Downloadable. Linking engine 405 is implementable in a static or configurable manner in accordance, for example, with characteristics of a particular user device/process stored intermittently or more persistently in storage 404. Linking engine 405 can also provide for restoring a Downloadable, such as a compressed, encrypted or otherwise encoded file that has been decompressed, decrypted or otherwise decoded via detection processing
20 (e.g. see FIG. 6b).

It is discovered, for example, that the manner in which the Windows OS initiates a binary executable or an ActiveX control can be utilized to enable protected initiation of a detected-Downloadable. Linking engine 405 is, for example, configurable to form, for

an ordinary single-executable Downloadable (e.g. an application program, applet, etc.) a sandboxed package 340 as a concatenation of ordered elements including an MPC 341, applicable policies 342 and the Downloadable or "XEQ" 343 (e.g. see FIG. 4).

Linking engine 405 is also configurable to form, for a Downloadable received by
 5 a server as a compressed single or multiple-executable Downloadable such as a zipped or meta file, a protecting package 340 including one or more MPCs, applicable policies and the one or more included executables of the Downloadable. For example, a sandboxed package can be formed in which a single MPC and policies precede and thus will affect all such executables as a result of inflating and installation. An MPC and applicable
 10 policies can also, for example, precede each executable, such that each executable will be separately sandboxed in the same or a different manner according to MPC/policy configuration (see above) upon inflation and installation. (See also FIGS. 5 and 6)

Linking engine is also configurable to form an initial MPC, MPC-policy or sandboxed package (e.g. prior to upon receipt of a downloadable) or an additional MPC,
 15 MPC-policy or sandboxed package (e.g. upon or following receipt of a downloadable), such that suitable MPCs/policies can be provided to a Downloadable-destination or other destination in a more distributed manner. In this way, requisite bandwidth or destination resources can be minimized (via two or more smaller packages) in compromise with latency or other considerations raised by the additional required communication.

20 A configurable linking engine can also be utilized in accordance with other requirements of particular devices/processes, further or different elements or other permutations in accordance with the teachings herein. (It might, for example be desirable to modify the ordering of elements, to provide one or more elements separately, to

provide additional information, such as a header, etc., or perform other processing in accordance with a particular device, protocol or other application considerations.)

Policy/authentication reader-analyzer 481 summarily depicts other protection mechanisms that might be utilized in conjunction with Downloadable detection, such as already discussed, and that can further be configurable to operate in accordance with policies or parameters (summarily depicted by security/authentication policies 482). Integration of such further protection in the depicted configuration, for example, enables a potential-Downloadable from a known unfriendly source, a source failing authentication or a provided-source that is confirmed to be fictitious to be summarily discarded, otherwise blocked, flagged, etc. (with or without further processing). Conversely, a potential-Downloadable from a known friendly source (or one confirmed as such) can be transferred with or without further processing in accordance with particular application considerations. (Other configurations including pre or post Downloadable detection mechanisms might also be utilized.)

Finally, transfer engine 406 of protection agent engine 303 provides for receiving and causing linking engine 405 (or other protection) results to be transferred to a destination user device/process. As depicted, transfer engine 406 is configured to receive and transfer a Downloadable, a determined non-executable or a sandboxed package. However, transfer engine 406 can also be provided in a more configurable manner, such as was already discussed for other system 400 elements. (Any one or more of system 400 elements might be configurably implemented in accordance with a particular application.) Transfer engine 406 can perform such transfer, for example, by adding the information to a server transfer queue (not shown) or utilizing another suitable method.

Turning to FIG. 5 with reference to FIG. 4, a code detector 421 example is illustrated in accordance with an embodiment of the invention. As shown, code detector 421 includes data fetcher 501, parser 502, file-type detector 503, inflater 504 and control 506; other depicted elements. While implementable and potentially useful in certain instances, are found to require substantial overhead, to be less accurate in certain instances (see above) and are not utilized in a present implementation; these will be discussed separately below. Code detector elements are further configurable in accordance with stored parameters retrievable by data fetcher 501. (A coupling between data fetcher 501 and control 506 has been removed for clarity sake.)

Data fetcher 501 provides for retrieving a potential-Downloadable or portions thereof stored in buffer 407 or parameters from storage 404, and communicates such information or parameters to parser 502. Parser 502 receives a potential-Downloadable or portions thereof from data fetcher 501 and isolates potential-Downloadable elements, such as file headers, source, destination, certificates, etc. for use by further processing elements.

File type detector 502 receives and determines whether the potential-Downloadable (likely) is or includes an executable file type. File-reader 502 can, for example, be configured to analyze a received potential-Downloadable for a file header, which is typically included in accordance with conventional data transfer protocols, such as a portable executable or standard “.exe” file format for Windows OS application programs, a Java class header for Java applets, and so on for other applications, distributed components, etc. “Zipped”, meta or other compressed files, which might include one or more executables, also typically provide standard single or multi-level

headers that can be read and used to identify included executable code (or other included information types). File type detector 502 is also configurable for analyzing potential-Downloadables for all potential file type delimiters or a more limited subset of potential file type delimiters (e.g. “.exe” or “.com” in conjunction with a DOS or Microsoft Windows OS Downloadable-destination).

Known file type delimiters can, for example, be stored in a more temporary or more persistent storage (e.g. storage 404 of FIG. 4) which file type detector 502 can compare to a received potential-Downloadable. (Such delimiters can thus also be updated in storage 404 as a new file type delimiter is provided, or a more limited subset of delimiters can also be utilized in accordance with a particular Downloadable-destination or other considerations of a particular application.) File type detector 502 further transfers to controller 506 a detected file type indicator indicating that the potential-Downloadable includes or does not include (i.e. or likely include) an executable file type.

In this example, the aforementioned detection processor is also included as pre-detection processor or, more particularly, a configurable file inflator 504. File inflator 504 provides for opening or “inflating” compressed files in accordance with a compressed file type received from file type detector 503 and corresponding file opening parameters received from data fetcher 501. Where a compressed file (e.g. a meta file) includes nested file type information not otherwise reliably provided in an overall file header or other information, inflator 504 returns such information to parser 502. File inflator 504 also provides any now-accessible included executables to control 506 where one or more included files are to be separately packaged with an MPC or policies.

Control 506, in this example, operates in accordance with stored parameters and provides for routing detected non-Downloadables or Downloadables and control information, and for conducting the aforementioned distributed downloading of packages to Downloadable-destinations. In the case of a non-Downloadable, for example, control

5 506 sends the non-Downloadable to transfer engine 406 (FIG. 4) along with any indicators that might apply. For an ordinary single-executable Downloadable, control 506 sends control information to agent generator 431 and the Downloadable to linking engine 405 along with any other applicable indicators (see 641 of FIG. 6b). Control 506 similarly handles a compressed single-executable Downloadable or a multiple

10 downloadable to be protected using a single sandboxed package. For a multiple-executable Downloadable, control 506 sends control information for each corresponding executable to agent generator agent generator 431, and sends the executable to linking engine 405 along with controls and any applicable indicators, as in 643b of FIG. 6b. (The above assumes, however, that distributed downloading is not utilized; when used –

15 according to applicable parameters- control 506 also operates in accordance with the following.)

Control 506 conducts distributed protection (e.g. distributed packaging) by providing control signals to agent generator 431, linking engine 405 and transfer engine 406. In the present example, control 506 initially sends controls to agent generator 431

20 and linking engine 405 (FIG. 4) causing agent generator to generate an initial MPC and initial policies, and sends control and a detected-Downloadable to linking engine 405. Linking engine 405 forms an initial sandboxed package, which transfer engine causes (in conjunction with further controls) to be downloaded to the Downloadable destination

(643a of FIG. 6b). An initial MPC within the sandboxed package includes an installer and a communicator and performs installation as indicated below. The initial MPC also communicates via the communicator controls to control 506 (FIG. 5) in response to which control 506 similarly causes generation of MPC-M and policy-M modules 643c, which linking engine 405 links and transfer engine 406 causes to be sent to the Downloadable destination, and so on for any further such modules.

(It will be appreciated, however, that an initial package might be otherwise configured or sent prior to receipt of a Downloadable in accordance with configuration parameters or user interaction. Information can also be sent to other user devices, such as that of an administrator. Further MPCs/policies might also be coordinated by control 506 or other elements, or other suitable mechanisms might be utilized in accordance with the teachings herein.)

Regarding the remaining detection engine elements illustrated in FIG. 5, where content analysis is utilized, parser 502 can also provide a Downloadable or portions thereof to content detector 505. Content detector 505 can then provide one or more content analyses. Binary detector 551, for example, performs detection of binary information; pattern detector 552 further analyzes the Downloadable for patterns indicating executable code, or other detectors can also be utilized. Analysis results therefrom can be used in an absolute manner, where a first testing result indicating executable code confirms Downloadable detection, which result is then sent to control 506. Alternatively, however, composite results from such analyses can also be sent to control 506 for evaluation. Control 506 can further conduct such evaluation in a summary manner (determining whether a Downloadable is detected according to a

majority or minimum number of indicators), or based on a weighting of different analysis results. Operation then continues as indicated above. (Such analysis can also be conducted in accordance with aspects of a destination user device or other parameters.)

FIG. 6a illustrates more specific examples of indicators/parameters and known (or “knowledge base”) elements that can be utilized to facilitate the above-discussed system 400 configurability and detection. For clarity sake, indicators, parameters and knowledge base elements are combined as indicated “parameters.” It will be appreciated, however, that the particular parameters utilized can differ in accordance with a particular application, and indicators, parameters or known elements, where utilized, can vary and need not correspond exactly with one another. Any suitable explicit or referencing list, database or other storage structure(s) or storage structure configuration(s) can also be utilized to implement a suitable user/device based protection scheme, such as in the above examples, or other desired protection schema.

Executable parameters 601 comprise, in accordance with the above examples, executable file type parameters 611, executable code parameters 612 and code pattern parameters 613 (including known executable file type indicators, header/code indicators and patterns respectively, where code patterns are utilized). Use parameters 602 further comprise user parameters 621, system parameters 622 and general parameters 623 corresponding to one or more users, user classifications, user-system correspondences or destination system, device or processes, etc. (e.g. for generating corresponding MPCs/policies, providing other protection, etc.). The remaining parameters include interface parameters 631 for providing MPC/policy (or further) configurability in

accordance with a particular device or for enabling communication with a device user (see below), and other parameters 632.

FIG. 6b illustrates a linking engine 405 according to an embodiment of the invention. As already discussed, linking engine 405 includes a linker for combining
 5 MPCs, policies or agents via concatenation or other suitable processing in accordance with an OS, JVM or other host executor or other applicable factors that might apply. Linking engine 405 also includes the aforementioned post-detection processor which, in this example, comprises a compressor 508. As noted, compressor 508 receives linked
 10 elements from linker 507 and, where a potential-Downloadable corresponds to a compressed file that was inflated during detection, re-forms the compressed file. (Known file information can be provided via configuration parameters, substantially reversal of inflating or another suitable method.) Encryption or other post-detection processing can also be conducted by linking engine 508.

FIGS. 7a, 7b and 8 illustrate a “sandbox protection” system, as operable within a
 15 receiving destination-device, according to an embodiment of the invention.

Beginning with FIG. 7a, a client 146 receiving sandbox package 340 will “recognize” sandbox package 340 as a (mobile) executable and cause a mobile code
 installer 711 (e.g. an OS loader, JVM, etc.) to be initiated. Mobile code installer 711 will also recognize sandbox package 340 as an executable and will attempt to initiate sandbox
 20 package 340 at its “beginning.” Protection engine 400 processing corresponding to destination 700 use of a such a loader, however, will have resulted in the “beginning” of sandbox package 340 as corresponding to the beginning of MPC 341, as noted with regard to the above FIG. 4 example.

Such protection engine processing will therefore cause a mobile code installer (e.g. OS loader 711, for clarity sake) to initiate MPC 341. In other cases, other processing might also be utilized for causing such initiation or further protection system operation. Protection engine processing also enables MPC 341 to effectively form a protection “sandbox” around Downloadable (e.g. detected-Downloadable or “XEQ”) 343, to monitor Downloadable 343, intercept determinable Downloadable 343 operation (such as attempted accesses of Downloadable 343 to destination resources) and, if “malicious”, to cause one or more other operations to occur (e.g. providing an alert, offloading the Downloadable, offloading the MPC, providing only limited resource access, possibly in a particular address space or with regard to a particularly “safe” resource or resource operation, etc.).

MPC 341, in the present OS example, executes MPC element installation and installs any policies, causing MPC 341 and protection policies 342 to be loaded into a first memory space, P1. MPC 341 then initiates loading of Downloadable 343. Such Downloadable initiation causes OS loader 711 to load Downloadable 343 into a further working memory space-P2 703 along with an API import table (“IAT”) 731 for providing Downloadable 631 with destination resource access capabilities. It is discovered, however that the IAT can be modified so that any call to an API can be redirected to a function within the MPC. The technique for modifying the IAT is documented within the MSDN (Microsoft Developers Network) Library CD in several articles. The technique is also different for each operating system (e.g. between Windows 9x and Windows NT), which can be accommodated by agent generator configurability, such as that given above.

MPC 341 therefore has at least initial access to API IAT 731 of Downloadable 632, and provides for diverting, evaluating and responding to attempts by Downloadable 632 to utilize system APIs 731, or further in accordance with protection policies 342.

In addition to API diverting, MPC 341 can also install filter drivers, which can be used

5 for controlling access to resources such as a Downloadable-destination file system or registry. Filter driver installation can be conducted as documented in the MSDN or using other suitable methods.

Turning to FIG. 8 with reference to FIG. 7b, an MPC 341 according to an embodiment of the invention includes a package extractor 801, executable installer 802, 10 sandbox engine installer 803, resource access diverter 804, resource access (attempt) analyzer 805, policy enforcer 806 and MPC de-installer 807. Package extractor 801 is initiated upon initiation of MPC 341, and extracts MPC 341 elements and protection policies 342. Executable installer 802 further initiates installation of a Downloadable by extracting the downloadable from the protected package, and loading the process into 15 memory in suspended mode (so it only loads into memory, but does not start to run). Such installation further causes the operating system to initialize the Downloadable's IAT 731 in the memory space of the downloadable process, P2, as already noted.

Sandbox engine installer 803 (running in process space P1) then installs the sandbox engine (803-805) and policies 342 into the downloadable process space P2. This 20 is done in different way in each operating system (e.g. see above). Resource access diverter 804 further modifies those Downloadable-API IAT entries that correspond with protection policies 342, thereby causing corresponding Downloadable accesses via Downloadable-API IAT 731 to be diverted resource access analyzer 805.

During Downloadable operation, resource access analyzer or “RAA” 805 receives and determines a response to diverted Downloadable (i.e. “malicious”) operations in accordance with corresponding protection policies of policies 342. (RAA 805 or further elements, which are not shown, can further similarly provide for other security mechanisms that might also be implemented.) Malicious operations can for example include, in a Windows environment: file operations (e.g. reading, writing, deleting or renaming a file), network operations (e.g. listen on or connect to a socket, send/receive data or view intranet), OS registry or similar operations (read/write a registry item), OS operations (exit OS/client, kill or change the priority of a process/thread, dynamically load a class library), resource usage thresholds (e.g. memory, CPU, graphics), etc.

Policy enforcer 806 receives RAA 805 results and causes a corresponding response to be implemented, again according to the corresponding policies. Policy enforcer 806 can, for example, interact with a user (e.g. provide an alert, receive instructions, etc.), create a log file, respond, cause a response to be transferred to the Downloadable using “dummy” or limited data, communicate with a server or other networked device (e.g. corresponding to a local or remote administrator), respond more specifically with a better known Downloadable, verify accessibility or user/system information (e.g. via local or remote information), even enable the attempted Downloadable access, among a wide variety of responses that will become apparent in view of the teachings herein.

The FIG. 9 flowchart illustrates a protection method according to an embodiment of the invention. In step 901, a protection engine monitors the receipt, by a server or other re-communicator of information, and receives such information intended for a

protected information-destination (i.e. a potential-Downloadable) in step 903. Steps 905-911 depict an adjunct trustworthiness protection that can also be provided, wherein the protection engine determines whether the source of the received information is known to be “unfriendly” and, if so, prevents current (at least unaltered) delivery of the potential-Downloadable and provides any suitable alerts. (The protection engine might also continue to perform Downloadable detection and nevertheless enable delivery or protected delivery of a non-Downloadable, or avoid detection if the source is found to be “trusted”, among other alternatives enabled by the teachings herein.)

If, in step 913, the potential-Downloadable source is found to be of an unknown or otherwise suitably authenticated/certified source, then the protection engine determines whether the potential-Downloadable includes executable code in step 915. If the potential-Downloadable does not include executable code, then the protection engine causes the potential-Downloadable to be delivered to the information-destination in its original form in step 917, and the method ends. If instead the potential-Downloadable is found to include executable code in step 915 (and is thus a “detected-Downloadable”), then the protection engine forms a sandboxed package in step 919 and causes the protection agent to be delivered to the information-Destination in step 921, and the method ends. As was discussed earlier, a suitable protection agent can include mobile protection code, policies and the detected-Downloadable (or information corresponding thereto).

The FIG. 10a flowchart illustrates a method for analyzing a potential-Downloadable, according to an embodiment of the invention. As shown, one or more aspects can provide useful indicators of the inclusion of executable code within the

potential-Downloadable. In step 1001, the protection engine determines whether the potential-Downloadable indicates an executable file type, for example, by comparing one or more included file headers for file type indicators (e.g. extensions or other descriptors). The indicators can be compared against all known file types executable by all protected Downloadable destinations, a subset, in accordance with file types executable or desirably executable by the Downloadable-destination, in conjunction with a particular user, in conjunction with available information or operability at the destination, various combinations, etc.

Where content analysis is conducted, in step 1003 of FIG. 10a, the protection engine analyzes the potential-Downloadable and determines in accordance therewith whether the potential-Downloadable does or is likely to include binary information, which typically indicates executable code. The protection engine further analyzes the potential-Downloadable for patterns indicative of included executable code in step 1003. Finally, in step 1005, the protection engine determines whether the results of steps 1001 and 1003 indicate that the potential-Downloadable more likely includes executable code (e.g. via weighted comparison of the results with a suitable level indicating the inclusion or exclusion of executable code). The protection engine, given a suitably high confidence indicator of the inclusion of executable code, treats the potential-Downloadable as a detected-Downloadable.

The FIG. 10b flowchart illustrates a method for forming a sandboxed package according to an embodiment of the invention. As shown, in step 1011, a protection engine retrieves protection parameters and forms mobile protection code according to the parameters. The protection engine further, in step 1013, retrieves protection parameters

and forms protection policies according to the parameters. Finally, in step 1015, the protection engine couples the mobile protection code, protection policies and received-information to form a sandboxed package. For example, where a Downloadable-destination utilizes a standard windows executable, coupling can further be accomplished via concatenating the MPC for delivery of MPC first, policies second, and received information third. (The protection parameters can, for example, include parameters relating to one or more of the Downloadable destination device/process, user, supervisory constraints or other parameters.)

The FIG. 11 flowchart illustrates how a protection method performed by mobile protection code ("MPC") according to an embodiment of the invention includes the MPC installing MPC elements and policies within a destination device in step 1101. In step 1102, the MPC loads the Downloadable without actually initiating it (i.e. for executables, it will start a process in suspended mode). The MPC further forms an access monitor or "interceptor" for monitoring or "intercepting" downloadable destination device access attempts within the destination device (according to the protection policies in step 1103, and initiates a corresponding Downloadable within the destination device in step 1105.

If, in step 1107, the MPC determines, from monitored/intercepted information, that the Downloadable is attempting or has attempted a destination device access considered undesirable or otherwise malicious, then the MPC performs steps 1109 and 1111; otherwise the MPC returns to step 1107. In step 1109, the MPC determines protection policies in accordance with the access attempt by the Downloadable, and in step 1111, the MPC executes the protection policies. (Protection policies can, for example, be retrieved from a temporary, e.g. memory/cache, or more persistent storage.)

As shown in the FIG. 12a example, the MPC can provide for intercepting Downloadable access attempts by a Downloadable by installing the Downloadable (but not executing it) in step 1201. Such installation will cause a Downloadable executor, such as a the Windows operating system, to provide all required interfaces and parameters (such as the IAT, process ID, etc.) for use by the Downloadable to access device resources of the host device. The MPC can thus cause Downloadable access attempts to be diverted to the MPC by modifying the Downloadable IAT, replacing device resource location indicators with those of the MPC (step 1203).

The FIG. 12b example further illustrates an example of how the MPC can apply suitable policies in accordance with an access attempt by a Downloadable. As shown, the MPC receives the Downloadable access request via the modified IAT in step 1211. The MPC further queries stored policies to determine a policy corresponding to the Downloadable access request in step 1213.

The foregoing description of preferred embodiments of the invention is provided by way of example to enable a person skilled in the art to make and use the invention, and in the context of particular applications and requirements thereof. Various modifications to the embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles, features and teachings disclosed herein. The embodiments described herein are not intended to be exhaustive or limiting. The present invention is limited only by the following claims.

WHAT IS CLAIMED IS:

1. A method, comprising:

receiving downloadable-information;

determining whether the downloadable-information includes executable code; and

5 causing mobile protection code to be communicated to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code.

10 2. The method of claim 1, wherein the receiving includes monitoring received information of an information re-communicator.

3. The method of claim 2, wherein the information re-communicator is a network server.

15 4. The method of claim 1, wherein the determining comprises analyzing the downloadable-information for an included type indicator indicating an executable file type.

5. The method of claim 1, wherein the determining comprises analyzing the downloadable-information for an included an included type detector indicating an archive
20 file that contains at least one executable.

6. The method of claim 1, wherein the determining comprises analyzing the downloadable-information for an included file type indicator and an information pattern

corresponding to one or more information patterns that tend to be included within
executable code.

7. The method of claim 1, further comprising receiving one or more executable code
5 characteristics of executable code that is capable of being executed by the information-
destination, and wherein the determining is conducted in accordance with the executable
code characteristics.

8. The method of claim 1, wherein the determining comprises performing one or more
10 analyses of the downloadable-information, the analyses producing detection-indicators
indicating whether a correspondence is detected between a downloadable-information
characteristic and at least one respective executable code characteristic, and evaluating
the detection-indicators to determine whether the downloadable-information includes
executable code.

9. The method of claim 8, wherein at least one of the detection-indicators indicates a
level of downloadable-information characteristic and executable code characteristic
correspondence.

10. The method of claim 8, wherein the evaluating includes assigning a weighted level of
20 importance to at least one of the indicators.

11. The method of claim 1, wherein the causing mobile protection code to be

communicated comprises forming a sandboxed package including the mobile protection code and the downloadable-information, and causing the sandboxed package to be communicated to the at least one information-destination.

- 5 12. The method of claim 10, wherein the sandboxed package is formed such that the mobile protection code will be executed by the information-destination before the downloadable-information.

00661229:051704
10 13. The method of claim 11, wherein the sandboxed package further includes protection policies according to which the mobile protection code is operable.

14. The method of claim 13, wherein the sandboxed package is formed for receipt by the information-destination such that the mobile protection code is received before the downloadable-information, and the downloadable information before the protection
15 policies.

15. The method of claim 13, wherein the protection policies correspond with at least one of the information-destination and a user of the information destination.

- 20 16. A system, comprising:

an information monitor for receiving downloadable-information;
a content inspection engine communicatively coupled to the information monitor for determining whether the downloadable-information includes executable code; and

a protection agent engine communicatively coupled to the content inspection engine for causing mobile protection code ("MPC") to be communicated to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code.

5

17. The system of claim 16, wherein the information monitor intercepts received information received by an information re-communicator.

18. The system of claim 17, wherein the information re-communicator is a network server.

19. The system of claim 16, wherein the content inspection engine comprises a file type detector for determining whether the downloadable-information includes a file type indicator indicating an executable file type.

20. The system of claim 16, wherein the content inspection engine comprises a parser for parsing the downloadable-information and a content analyzer communicatively coupled to the parser for determining whether one or more downloadable-information elements of the downloadable-information correspond with executable code elements are executable code elements.

21. The system of claim 16, wherein the content inspection engine comprises one or more downloadable-information analyzers for analyzing the downloadable-information,

each analyzer producing therefrom a detection indicator indicating whether a
downloadable-information characteristic corresponds with an executable code
characteristic, and an inspection controller communicatively coupled to the analyzers for
determining whether the indicators indicate that the downloadable-information includes
5 executable code.

22. The system of claim 21, wherein at least one of the detection-indicators indicates a
level of downloadable-information characteristic and executable code characteristic
correspondence.

23. The system of claim 21, wherein the evaluating includes assigning a weighted level
of importance to at least one of the detection-indicators.

24. The system of claim 16, wherein the sandboxed package engine comprises an MPC
generator for providing the MPC, a linking engine coupled to the MPC generator for
forming a protection agent including the MPC and the downloadable-information, and a
transfer engine for causing the protection agent to be communicated to the at least one
information-destination.

20 25. The system of claim 24, wherein the protection agent engine further comprises a
policy generator communicatively coupled to the linking engine for providing protection
policies according to which the MPC is operable.

26. The system of claim 25, wherein the sandboxed package is formed for receipt by the information-destination such that the mobile protection code is executed before the downloadable-information.

5 27. The system of claim 26, wherein the protection policies correspond with policies of at least one of the information-destination and a user of the information destination.

28. A system, comprising:

means for receiving downloadable-information;

10 means for determining whether the downloadable-information includes executable code; and

means for causing mobile protection code to be communicated to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code.

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

receiving downloadable-information;

determining whether the downloadable-information includes executable code; and

20 causing mobile protection code to be communicated to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code.

30. A method, comprising:

receiving, at an information re-communicator, downloadable-information,

including executable code; and

causing mobile protection code to be executed by a mobile code executor at a
5 downloadable-information destination such that one or more operations of the executable
code at the destination, if attempted, will be processed by the mobile protection code.

31. The method of claim 30, wherein the mobile code executor is a Java Virtual
Machine.

32. The method of claim 30, wherein the mobile code executor is the operating system,
running native code executables.

33. The method of claim 30, wherein the mobile code executor is ActiveX subsystem of
15 the windows operating system

34. The method of claim 30, wherein the mobile code executor is the Microsoft
Windows scripting host

20 35. The method of claim 30, wherein the causing is accomplished by forming a
sandboxed package including the mobile protection code and the downloadable-
information, and causing the sandboxed package to be delivered to the downloadable-
information destination.

36. The method of claim 35, wherein the sandboxed package further includes protection policies according to which the processing by the mobile protection code is conducted.

5 37. A sandboxed package formed according to the method of claim 35.

38. A sandboxed package formed according to the method of claim 36.

39. The method of claim 36, wherein the forming comprises generating the mobile protection code, generating the sandboxed package, and linking the mobile protection code, protection policies and downloadable-information.

40. The method of claim 39, wherein the generating of at least one of the mobile protection code and the protection policies is conducted in accordance with one or more destination-characteristics of the destination.

41. The method of claim 40, wherein the destination-characteristics include characteristics corresponding to at least one of a destination user, a destination device and a destination process.

42. The method of claim 35, wherein the causing the sandboxed package to be executed includes communicating the sandboxed package to a communication buffer of the information re-communicator.

43. The method of claim 30, wherein the re-communicator is at least one of a firewall and a network server.

5 44. The method of claim 30, wherein the sandboxed package has a same file type as the downloadable-information, thereby causing the mobile code executor to be unaware that the protected package is not a normal downloadable.

0961230 05170
10 45. The method of claim 44, wherein the sandboxed package is formed using concatenation of a mobile protection code, a policy, and a downloadable.

10 46. The method of claim 30, wherein executing the mobile protection code at the destination causes downloadable interfaces to resources at the destination to be modified such that at least one attempted operation of the executable code is diverted to the mobile protection code.

15 47. A system, comprising:
receiving means for receiving, at an information re-communicator, downloadable-information, including executable code; and
20 mobile code means communicatively coupled to the receiving means for causing mobile protection code to be executed by a mobile code executor at a downloadable-information destination such that one or more operations of the executable code at the destination, if attempted, will be processed by the mobile protection code.

48. The system of claim 47, wherein the mobile code executor is a Java Virtual Machine.

49. The system of claim 47, wherein the mobile code executor is an operating system,
5 running native code executables.

50. The system of claim 47, wherein the mobile code executor is an ActiveX subsystem
of the windows operating system.

51. The system of claim 47, wherein the mobile code executor is a Microsoft Windows
10 scripting host.

52. The system of claim 47, wherein the causing is accomplished by forming a
sandboxed package including the mobile protection code and the downloadable-
15 information, and causing the sandboxed package to be delivered to the downloadable-
information destination.

53. The system of claim 52, wherein the sandboxed package further includes protection
policies according to which the processing by the mobile protection code is conducted.

20 54. The system of claim 53, wherein the forming comprises generating the mobile
protection code, generating the protection policies, and linking the mobile protection
code, protection policies and downloadable-information.

55. The system of claim 54, wherein the generating of at least one of the mobile protection code and the protection policies is conducted in accordance with one or more destination-characteristics of the destination.

5

56. The system of claim 55, wherein the destination-characteristics include characteristics corresponding to at least one of a destination user, a destination device and a destination process.

00661229:054701
T02F50:0229860

57. The system of claim 46, wherein the causing the sandboxed package to be executed includes communicating the sandboxed package to a communication buffer of the information re-communicator.

58. The system of claim 47, wherein the re-communicator is at least one of a firewall and a network server.

15

59. The system of claim 47, wherein executing the mobile protection code at the destination causes downloadable interfaces a resource at the destination to be modified such that at least one attempted operation of the executable code is diverted to the mobile protection code.

20

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

receiving, at an information re-communicator, downloadable-information,
including executable code; and

causing mobile protection code to be executed by a mobile code executor at a
downloadable-information destination such that one or more operations of the executable
5 code at the destination, if attempted, will be processed by the mobile protection code.

61. A method, comprising:

receiving mobile protection code ("MPC") and a Downloadable at a
Downloadable-destination;

10 causing, by the MPC, one or more operations attempted by the Downloadable to
be received by the MPC;

receiving, by the MPC, an attempted operation of the Downloadable; and
initiating, by the MPC, a protection policy corresponding to the attempted
operation.

15 62. The method of claim 61, wherein the receiving comprises receiving a sandboxed
package that includes the MPC, the Downloadable and one or more protection policies.

63. The method of claim 62, wherein the sandboxed package is configured such that the
20 MPC is executed first, the Downloadable is executed by the MPC and the protection
policies are accessible to the MPC.

64. The method of claim 61, wherein the causing comprises modifying, by the MPC,

interfaces of a corresponding downloadable to resources at the destination.

65. The method of claim 64, wherein the modifying is accomplished by initiating a loading of the Downloadable, thereby causing a mobile code executor to provide and initialize the interfaces, modifying one or more interface elements to divert corresponding attempted Downloadable operations to the MPC, and initiating execution of the Downloadable.

66. The method of claim 64, wherein the interfaces comprise an import address table ("IAT") of a native code executable downloadable.

67. The method of claim 64, wherein modifying the interfaces installs a filter-driver between the downloadable and the resources.

68. A system, comprising:

a mobile code executor for initiating received mobile code; and

a sandboxed package capable of being received and initiated by the mobile code executor, the sandboxed package including a Downloadable and mobile protection code ("MPC") for causing one or more Downloadable operations to be intercepted and for processing the intercepted operations, if the Downloadable attempts to initiate the operations.

69. The system of claim 60, wherein the MPC comprises:

an MPC installer for causing MPC elements to be installed;

a Downloadable installer communicatively coupled to the MPC element installer
for installing the Downloadable;

a resource access diverter communicatively coupled to the MPC installer for
5 causing the Downloadable operations to be intercepted;

a resource access analyzer communicatively coupled to the MPC installer for
receiving an intercepted Downloadable operation and determining a protection policy
corresponding to the intercepted Downloadable operation; and

0961230 05170
10 a policy enforcer communicatively coupled to the resource access analyzer for
processing the intercepted Downloadable operation.

70. The system of claim 69, wherein the resource access diverter modifies one or more
elements of an interface usable by the Downloadable to effectuate the Downloadable
operations.

71. The system of claim 69, wherein the mobile code executor is a Java Virtual Machine.

72. The system of claim 69, wherein the mobile code executor is an operating system,
running native code executables.

20

73. The system of claim 69, wherein the mobile code executor is an ActiveX subsystem
of the windows operating system.

74. The system of claim 69, wherein the mobile code executor is an Microsoft Windows scripting host.

75. A system, comprising

- 5 receiving means for receiving mobile protection code ("MPC") and a Downloadable at a Downloadable-destination;
- monitoring means for causing, by the MPC, one or more operations attempted by the Downloadable to be received by the MPC;
- 10 second receiving means receiving, by the MPC, an attempted operation of the Downloadable; and
- initiating means for initiating, by the MPC, a protection policy corresponding to the attempted operation.

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

- 15 receiving mobile protection code ("MPC") and a Downloadable at a Downloadable-destination;
- causing, by the MPC, one or more operations attempted by the Downloadable to be received by the MPC;
- 20 receiving, by the MPC, an attempted operation of the Downloadable; and
- initiating, by the MPC, a protection policy corresponding to the attempted operation.

ABSTRACT OF THE DISCLOSUREMALICIOUS MOBILE CODE RUNTIME MONITORING
SYSTEM AND METHODS

5

Protection systems and methods provide for protecting one or more personal computers ("PCs") and/or other intermittently or persistently network accessible devices or processes from undesirable or otherwise malicious operations of Java™ applets, ActiveX™ controls, JavaScript™ scripts, Visual Basic scripts, add-ins, downloaded/10 uploaded programs or other "Downloadables" or "mobile code" in whole or part. A protection engine embodiment provides, within a server, firewall or other suitable "re-communicator," for monitoring information received by the communicator, determining whether received information does or is likely to include executable code, and if so, causes mobile protection code (MPC) to be transferred to and rendered operable within a15 destination device of the received information, more suitably by forming a protection agent including the MPC, protection policies and a detected-Downloadable. An MPC embodiment further provides, within a Downloadable-destination, for initiating the Downloadable, enabling malicious Downloadable operation attempts to be received by the MPC, and causing (predetermined) corresponding operations to be executed in20 response to the attempts, more suitably in conjunction with protection policies.

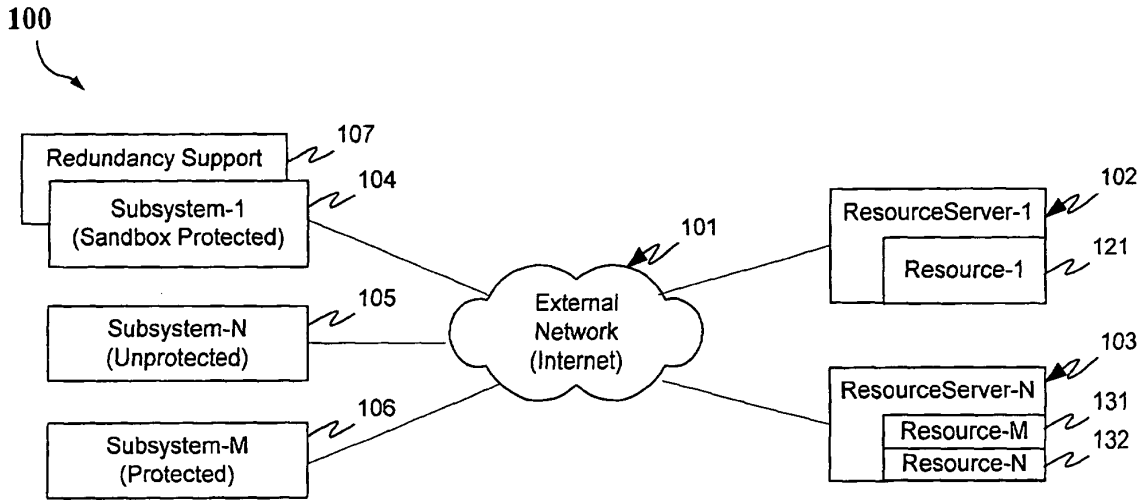


FIG. 1a

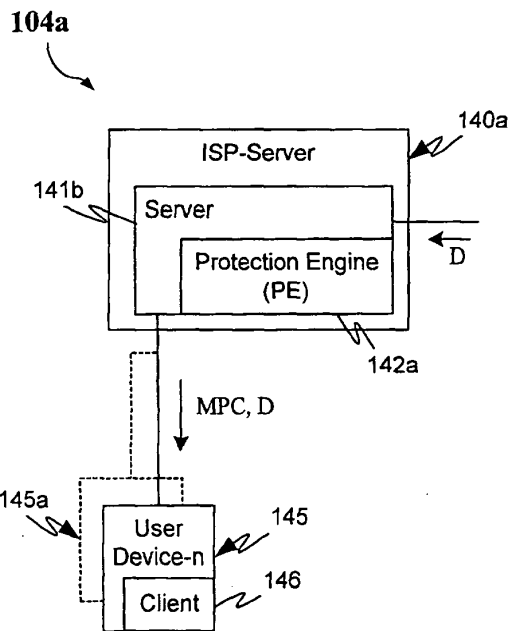


FIG. 1b

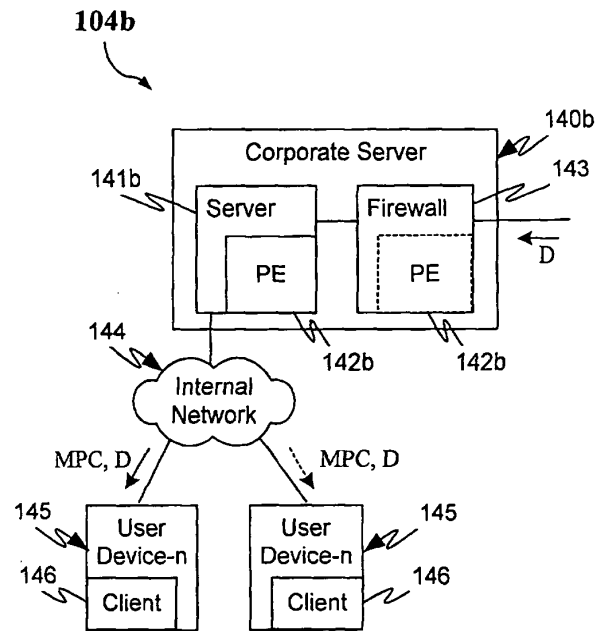


FIG. 1c

Malicious Mobile Code Runtime Monitoring
System and Methods
Inventor: Yigal Eder, et al.

FIG. 2

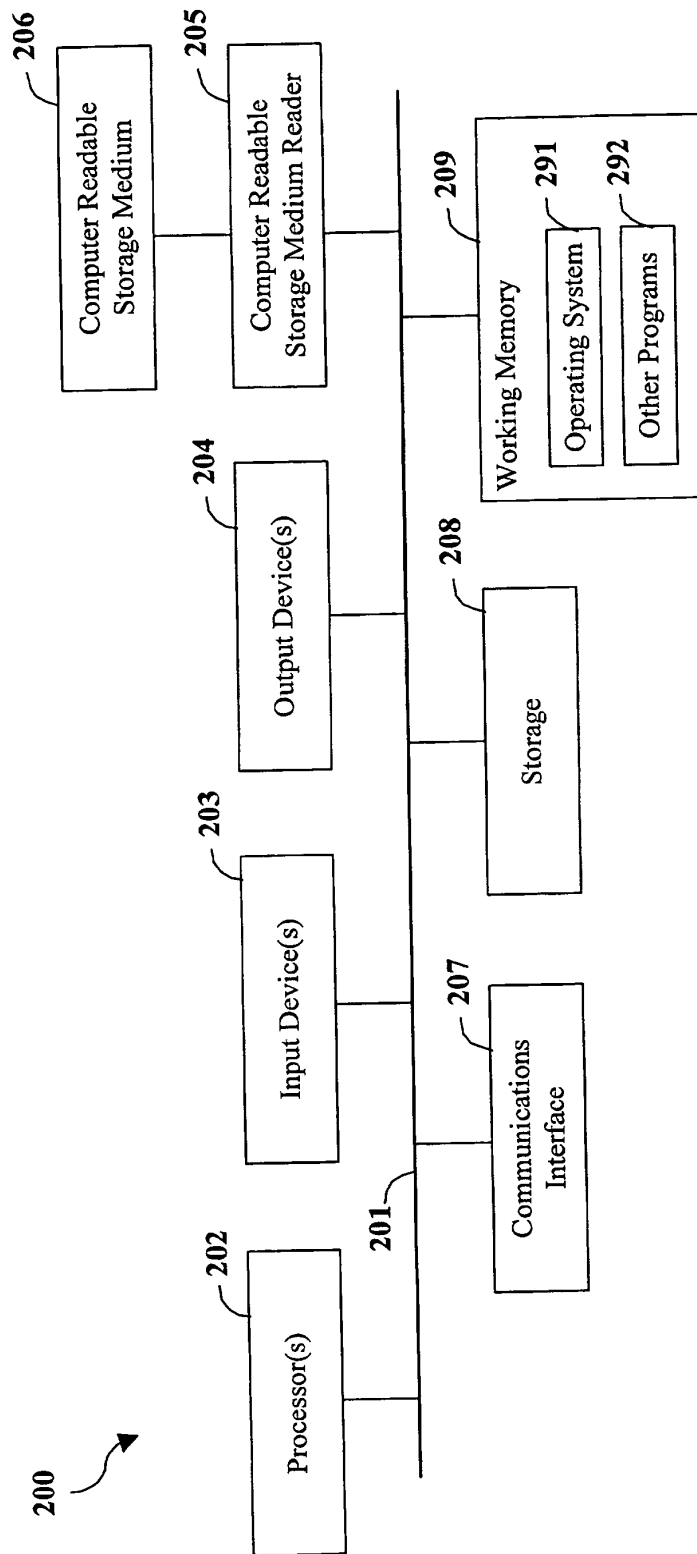


FIG. 2

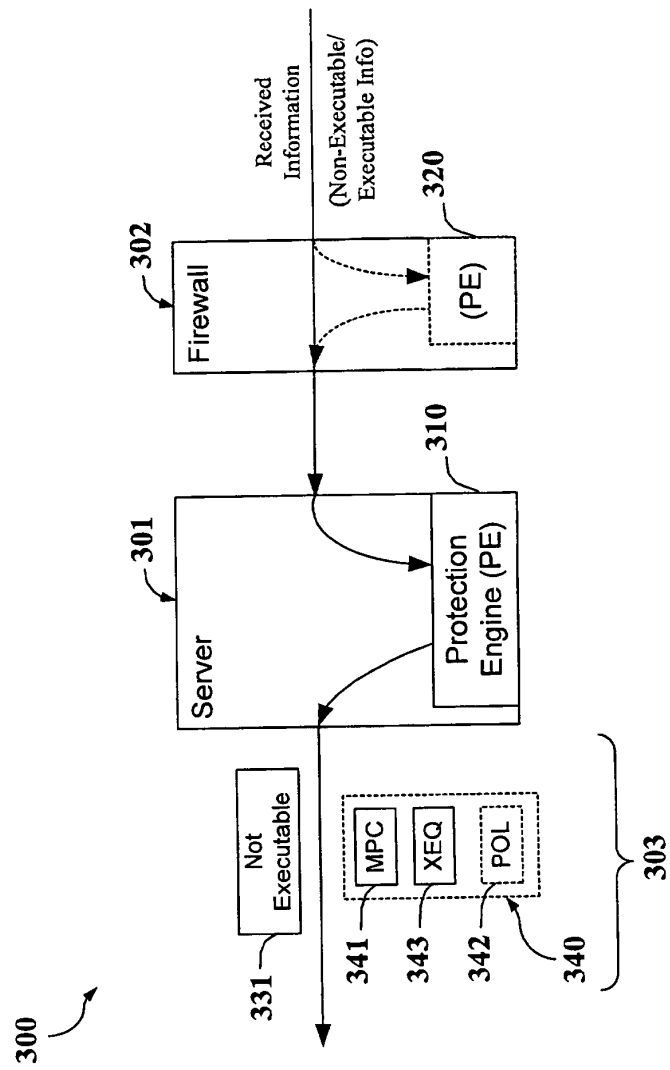


FIG. 3

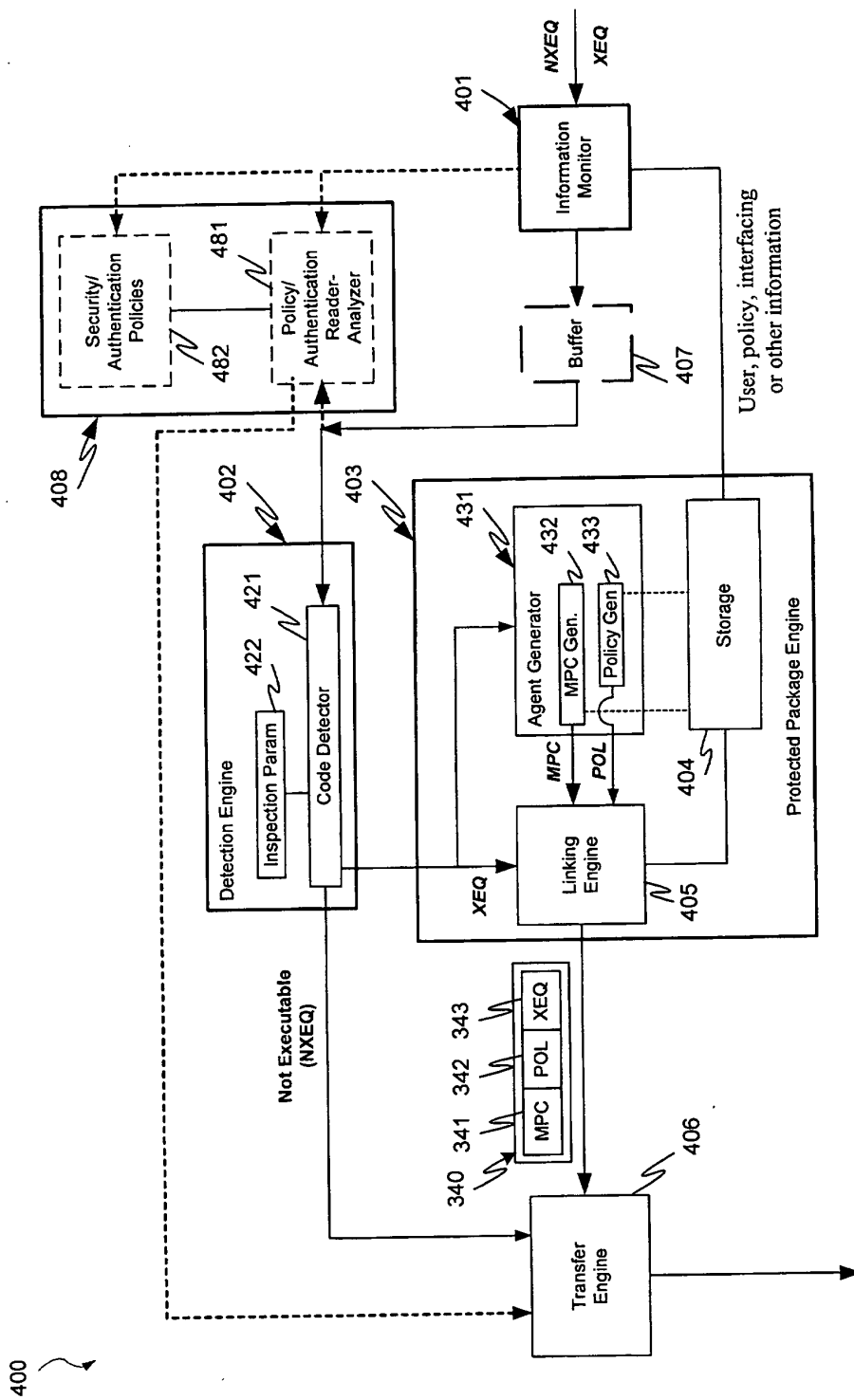


FIG. 4

FIG. 5

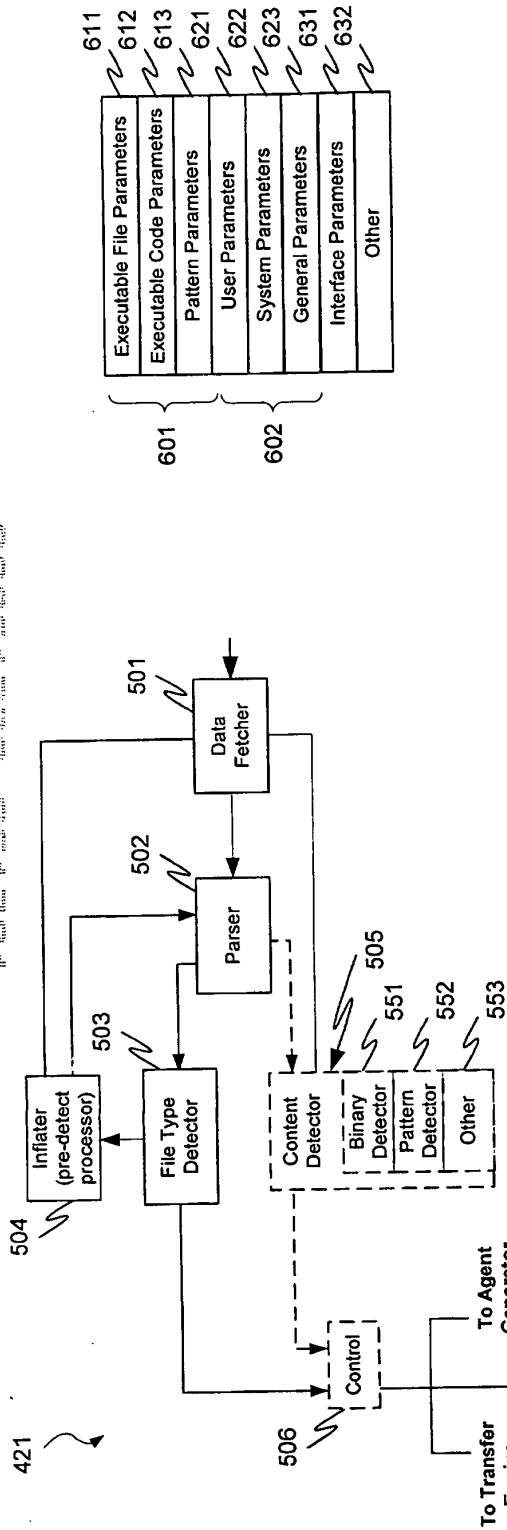


FIG. 5

FIG. 6a

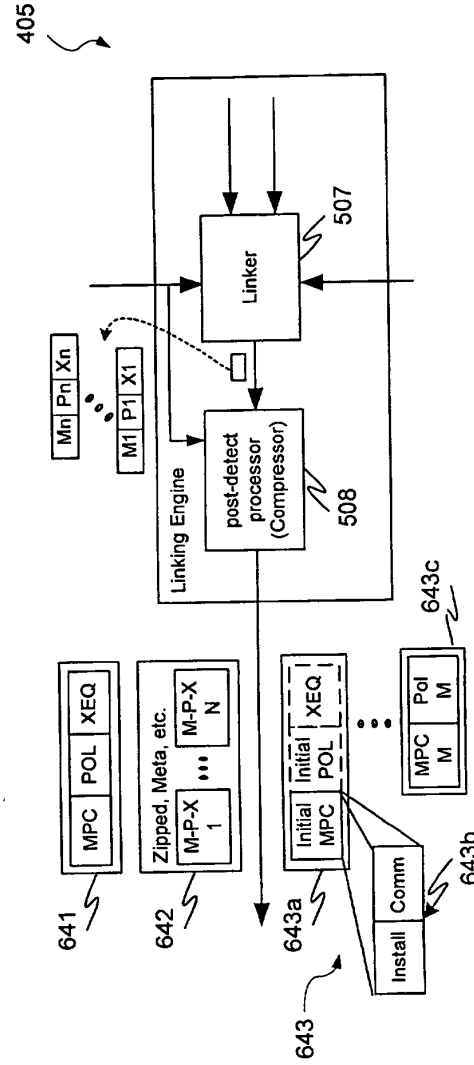
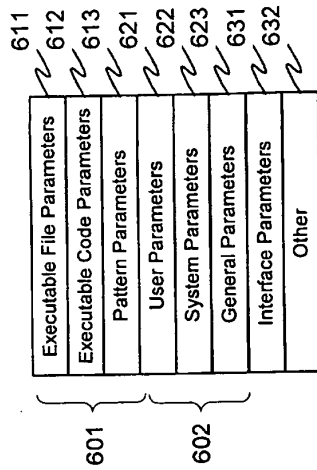


FIG. 6b

700

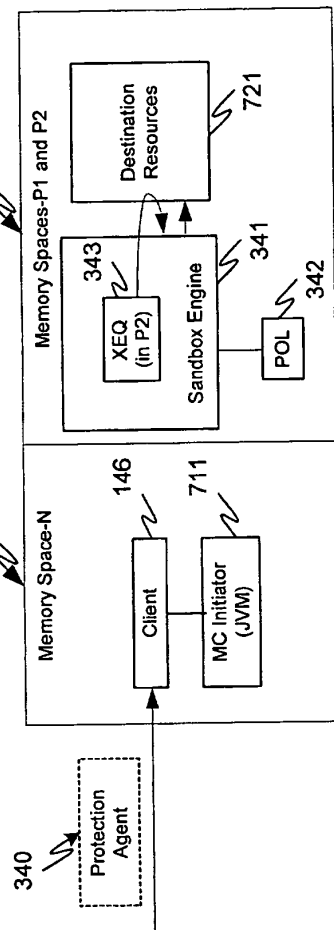


FIG. 7a

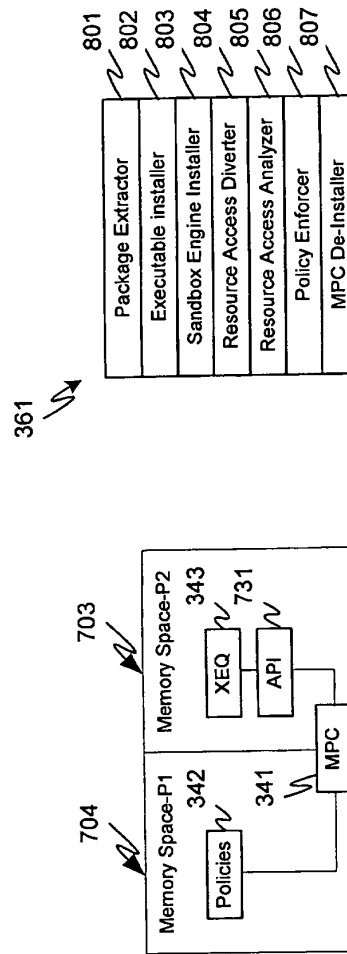


FIG. 8

FIG. 7b

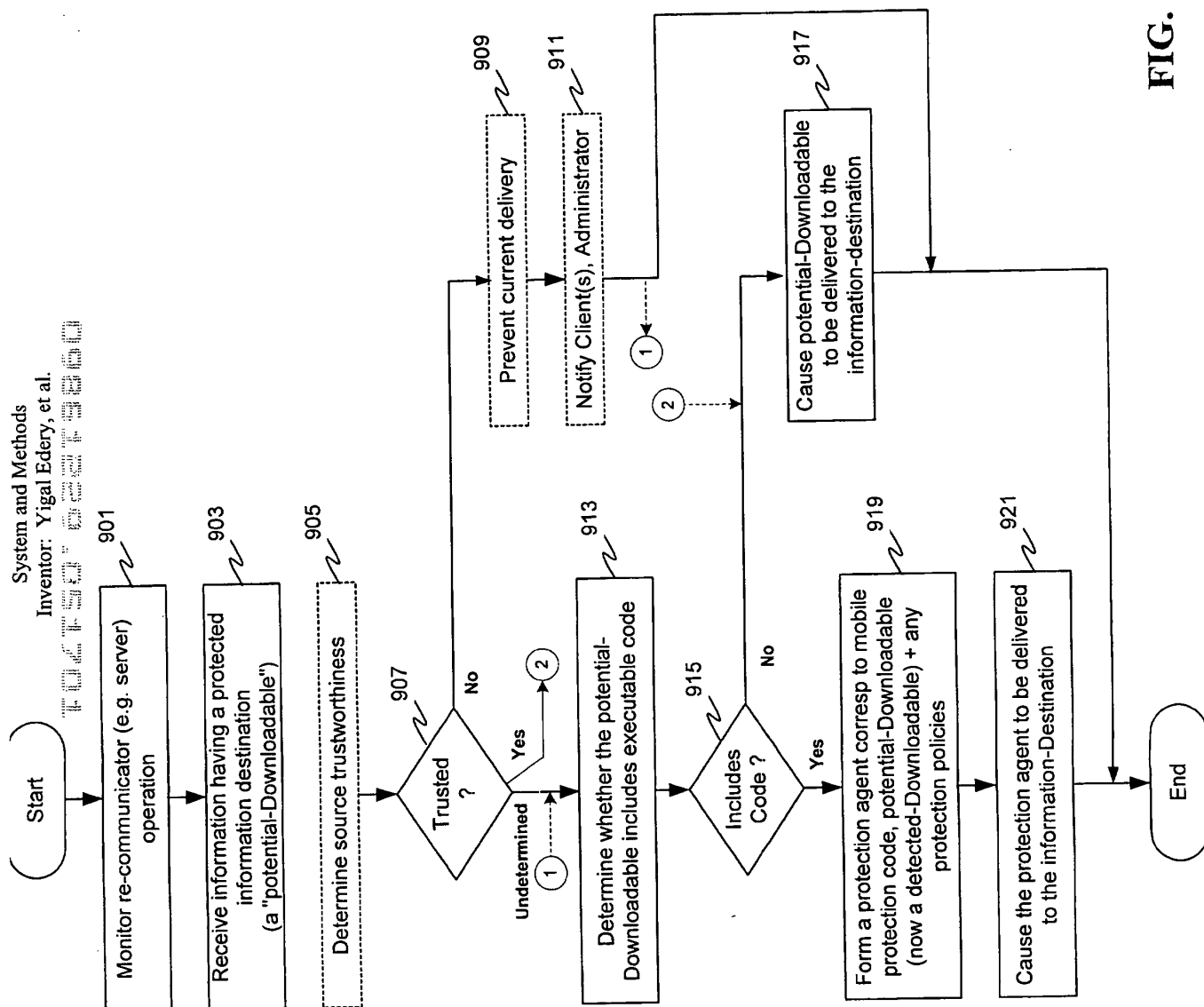


FIG. 9

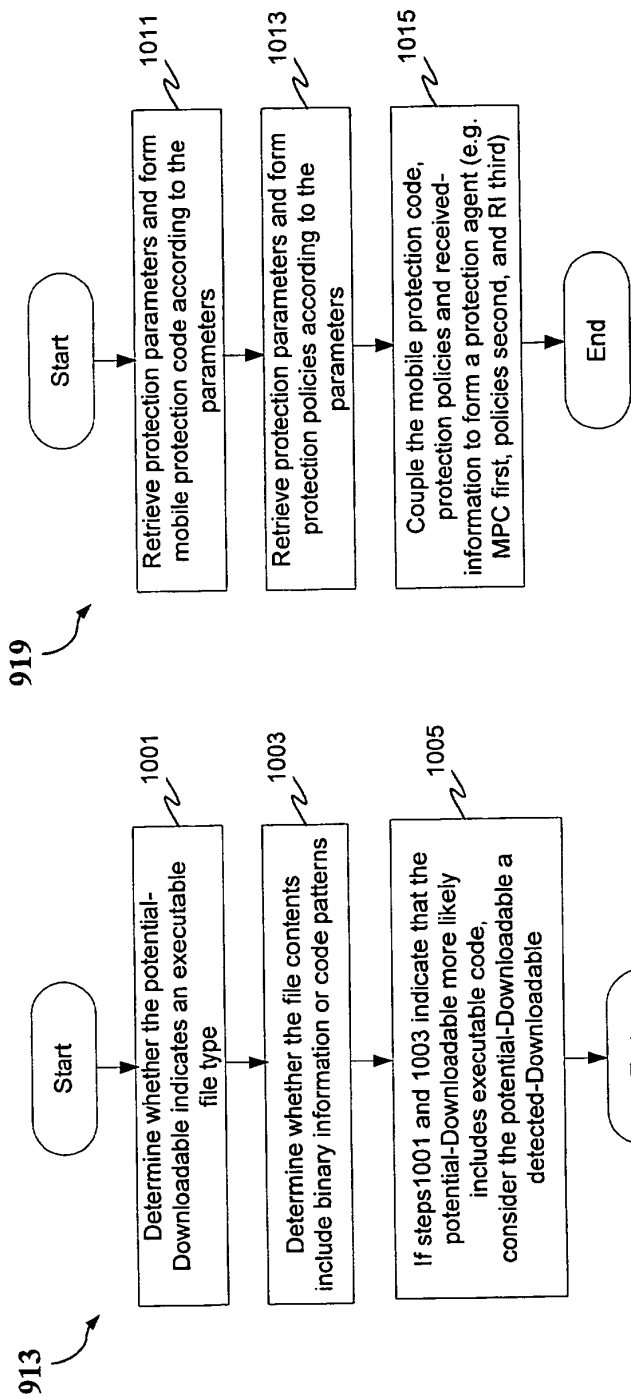


FIG. 10A

FIG. 10B

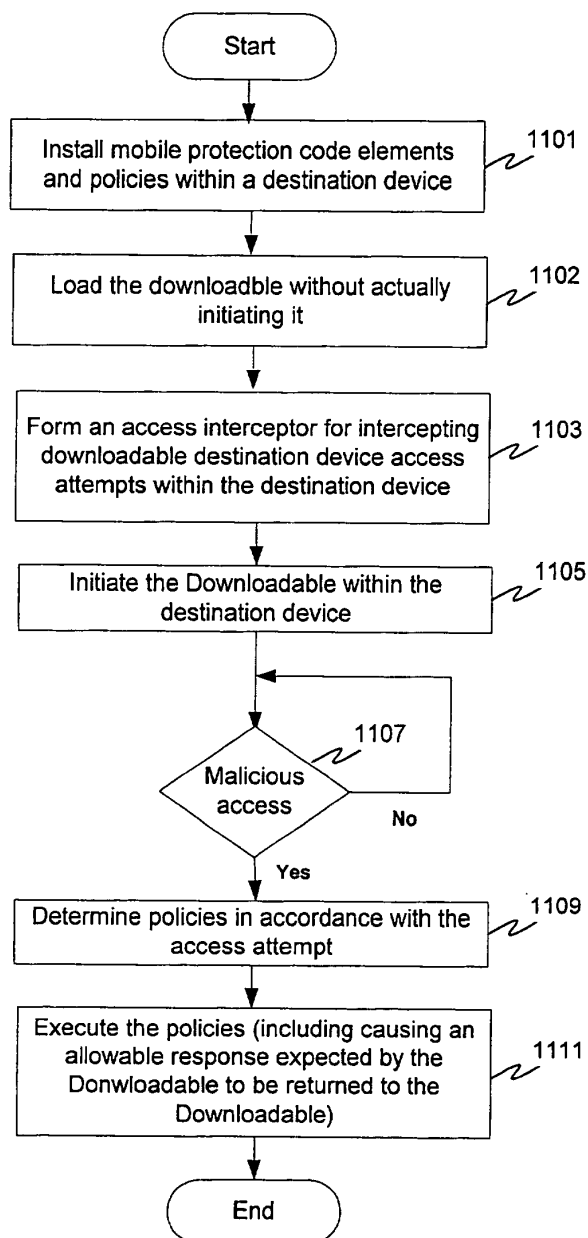


FIG. 11

FIG. 1103

1103

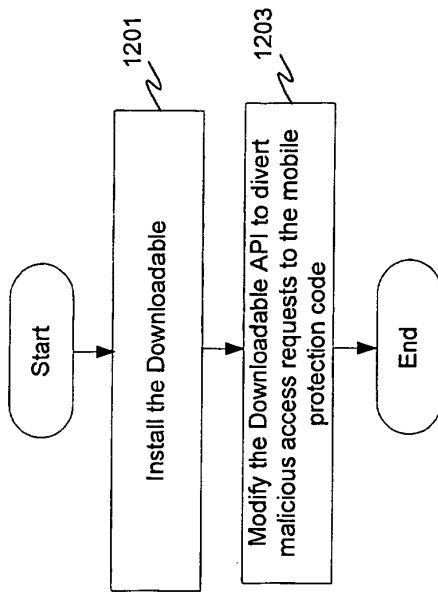


FIG. 12a

1109

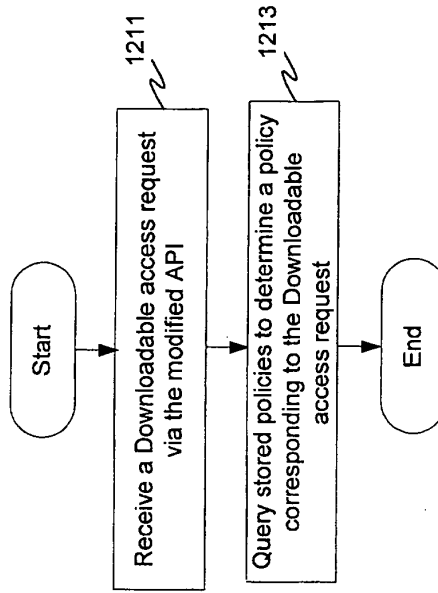


FIG. 12b



**DECLARATION FOR UTILITY OR
DESIGN
PATENT APPLICATION
(37 CFR 1.63)**

☐ Declaration Submitted With Initial Filing OR ☒ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number 43426.00014

First Named Inventor Yigal EDERY

COMPLETE IF KNOWN

Application Number 09/861,229

Filing Date May 17, 2001

Art Unit 2152

Examiner Name Unknown

I hereby declare that:

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

I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS

the specification of which (Title of the Invention)

☐ is attached hereto

OR

☒ was filed on (MM/DD/YYYY) 5/17/2001 as United States Application Number or PCT International

Application Number 09/861,229 and was amended on (MM/DD/YYYY) (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

[Page 1 of 3]

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 21 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.


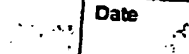
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Best Available Copy

PTO/SB/01 (08-08)

Approved for use through 07/31/2008. OMB 0851-0032
 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 contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

Direct all correspondence to:				<input checked="" type="checkbox"/> Customer Number		30258		OR		<input type="checkbox"/> Correspondence address below	
Name											
Address											
City				State				ZIP			
Country				Telephone				Fax			
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 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.											
NAME OF SOLE OR FIRST INVENTOR:						<input type="checkbox"/> A petition has been filed for this unsigned inventor					
Given Name (first and middle (if any))						Family Name or Surname					
Yigal Mordechai						EDERY					
Inventor's Signature						Date					
						17/4/2005					
Residence: City				State		Country		Citizenship			
Pardesia				N/A		Israel		Israel			
Mailing Address											
Hashikma 11, POB 1115											
City				State		Zip		Country			
Pardesia				N/A		42815		Israel			
NAME OF SECOND INVENTOR:						<input type="checkbox"/> A petition has been filed for this unsigned inventor					
Given Name (first and middle (if any))						Family Name or Surname					
Nimrod Itzhak						VERED					
Inventor's Signature						Date					
											
Residence: City				State		Country		Citizenship			
Goosh Tel-Mond				N/A		Israel		Israel			
Mailing Address											
Moshav Mismaret #81											
City				State		Zip		Country			
Goosh Tel-Mond				N/A		40695		Israel			
<input checked="" type="checkbox"/> Additional inventors or a legal representative are being named on the 1 supplemental sheet(s) PTO/SB/02A or 02LR attached hereto.											

[Page 2 of 3]

Best Available Copy

TOTAL P. 11


PTO/SB/01 (09-03)

Approved for use through 07/01/2005, OMB 0551-0032

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 contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

Direct all correspondence to: <input checked="" type="checkbox"/> Customer Number 30256 <input type="checkbox"/> OR <input type="checkbox"/> Correspondence address below			
Name			
Address			
City	State	ZIP	
Country	Telephone	Fax	
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 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.			
NAME OF SOLE OR FIRST INVENTOR:		<input type="checkbox"/> A petition has been filed for this unsigned inventor	
Given Name (first and middle (if any)) Yigal Mordechai		Family Name or Surname EDERY	
Inventor's Signature		Date	
Residence: City Pardesia	State N/A	Country Israel	Citizenship Israel
Mailing Address Hashikma 11, POB 1115			
City Pardesia	State N/A	Zip 42815	Country Israel
NAME OF SECOND INVENTOR:		<input type="checkbox"/> A petition has been filed for this unsigned inventor	
Given Name (first and middle (if any)) Nimrod Itzhak		Family Name or Surname VERED	
Inventor's Signature 		Date 19/5/05	
Residence: City Gosh Tel-Mond	State N/A	Country Israel	Citizenship Israel
Mailing Address Moshav Miameret #81			
City Gosh Tel-Mond	State N/A	Zip 40885	Country Israel
<input checked="" type="checkbox"/> Additional inventors or a legal representative are being named on the supplemental sheet(s) PTO/SB/02A or 02LR attached hereto.			

[Page 2 of 3]

Best Available Copy

MAY-11-2005 WED 08:50 AM

FAX NO. 97482036

P. 02

TOTAL P.02

PTO/SB/82A (85-64)

Approved for use through 07/31/2006. GWS 0551-0022
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Under the Password Protection Act of 1999, no person may knowingly or recklessly disclose or attempt to disclose information that is a trade secret or confidential information.

DECLARATION	ADDITIONAL INVENTOR(S) Supplemental Sheet	Page 3 of 3
--------------------	---	-------------

Name of Additional Inventor, if any				<input type="checkbox"/> A petition has been filed for this unsigned inventor	
Given Name (first and middle if any)			Family Name or Surname		
David R.			KROLL		
Inventor's Signature				Date May 8, 2005	
Residence: City	San Jose	State	CA	Country	USA
Mailing Address					
4050 Kingsbrook Drive					
Mailing Address					
City	San Jose	State	CA	Zip	95134
Country USA					
Name of Additional Inventor, if any				<input type="checkbox"/> A petition has been filed for this unsigned inventor	
Given Name (first and middle if any)			Family Name or Surname		
Shimon			TOURQUIL		
Inventor's Signature				Date MARCH 6, 2005	
Residence: City	Kefar-Haim	State	N/A	Country	Israel
Mailing Address					
Mailing Address					
City	Kefar-Haim	State	N/A	Zip	43946
Country Israel					
Name of Additional Inventor, if any				<input type="checkbox"/> A petition has been filed for this unsigned inventor	
Given Name (first and middle if any)			Family Name or Surname		
Inventor's Signature				Date	
Residence: City		State		Country	
Mailing Address					
Mailing Address					
City		State		Zip	
Country					

This collection of information is required by 35 U.S.C. 116 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to be (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 21 minutes to complete, including gathering, preparing, and submitting the complete 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 (1-800-766-9199) and select option 2.

00148674922036 P.02

TO

03-MAY-2005 11:33 FROM FINJRM SOFTWARE

Best Available Copy

May. 18 2005 03:54PM P2

FAX NO. :

FROM :

SOPHOS
EXHIBIT 1012 - PAGE 0079

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.

DECLARATION	ADDITIONAL INVENTOR(S) Supplemental Sheet
Page 3 of 3	

Name of Additional Inventor, if any				<input type="checkbox"/> A petition has been filed for this unsigned inventor	
Given Name (first and middle [if any])			Family Name or Surname		
David R.			KROLL		
Inventor's Signature				Date	
Residence: City	San Jose	State	CA	Country	USA
Mailing Address 4856 Kingbrook Drive					
Mailing Address					
City	San Jose	State	CA	ZIP	95124
Country USA					
Name of Additional Inventor, if any				<input type="checkbox"/> A petition has been filed for this unsigned inventor	
Given Name (first and middle [if any])			Family Name or Surname		
Shlomo			TOUBOUL		
Inventor's Signature				Date MARCH 6, 2005	
Residence: City	Kefar-Haim	State	N/A	Country	Israel
Mailing Address					
Mailing Address					
City	Kefar-Haim	State	N/A	Zip	42945
Country Israel					
Name of Additional Inventor, if any				<input type="checkbox"/> A petition has been filed for this unsigned inventor	
Given Name (first and middle [if any])			Family Name or Surname		
Inventor's Signature				Date	
Residence: City		State		Country	
Mailing Address					
Mailing Address					
City		State		Zip	
Country					

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 21 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 (1-800-786-9199) and select option 2.

Best Available Copy

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET							SERIAL NO.	FILING DATE
							APPLICANT(S)	
CLAIMS								
	AS FILED		AFTER 1ST AMENDMENT		AFTER 2ND AMENDMENT			
	IND	DEP	IND	DEP	IND	DEP	IND	DEP
1							51	
2							52	
3							53	
4							54	
5							55	
6							56	
7							57	
8							58	
9							59	
10							60	
11							61	
12							62	
13							63	
14							64	
15							65	
16							66	
17							67	
18							68	
19							69	
20							70	
21							71	
22							72	
23							73	
24							74	
25							75	
26							76	
27							77	
28							78	
29							79	
30							80	
31							81	
32							82	
33							83	
34							84	
35							85	
36							86	
37							87	
38							88	
39							89	
40							90	
41							91	
42							92	
43							93	
44							94	
45							95	
46							96	
47							97	
48							98	
49							99	
50							100	
TOTAL IND.							TOTAL IND.	
TOTAL DEP.							TOTAL DEP.	
TOTAL CLAIMS							TOTAL CLAIMS	

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET							SERIAL NO. 11370114	FILED DATE 03-07-06					
							APPLICANT(S)						
CLAIMS													
	AS FILED		AFTER 1ST AMENDMENT		AFTER 2ND AMENDMENT								
	IND	DEP	IND	DEP	IND	DEP		IND	DEP	IND	DEP	IND	DEP
101													
2													
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													
16													
17													
18													
19													
20													
21													
22													
23													
24													
25													
26													
27													
28													
29													
30													
31													
32													
33													
34													
35													
36													
37													
38													
39													
40													
41													
42													
43													
44													
45													
46													
47													
48													
49													
50													
TOTAL IND.													
TOTAL DEP.													
TOTAL CLAIMS													
51													
52													
53													
54													
55													
56													
57													
58													
59													
60													
61													
62													
63													
64													
65													
66													
67													
68													
69													
70													
71													
72													
73													
74													
75													
76													
77													
78													
79													
80													
81													
82													
83													
84													
85													
86													
87													
88													
89													
90													
91													
92													
93													
94													
95													
96													
97													
98													
99													
100													
TOTAL IND.													
TOTAL DEP.													
TOTAL CLAIMS													

151
76
75

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

03/10/2006 WASFAW1 00000060 503400 11370114

01 FC:1011	300.00 DA
02 FC:1111	500.00 DA
03 FC:1311	200.00 DA
04 FC:1201	3600.00 DA
05 FC:1202	2750.00 DA

PTO-1556
(5/87)

*U.S. Government Printing Office: 2002 — 498-267/88033

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.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875 Effective December 8, 2004

Application or Docket Number

11370114

APPLICATION AS FILED - PART I

(Column 1)

(Column 2)

SMALL ENTITY

OR

OTHER THAN
SMALL ENTITY

FOR	NUMBER FILED	NUMBER EXTRA
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A
SEARCH FEE (37 CFR 1.16(d), (f), or (m))	N/A	N/A
EXAMINATION FEE (37 CFR 1.16(e), (g), or (q))	N/A	N/A
TOTAL CLAIMS (37 CFR 1.16(i))	75 minus 20 =	55
INDEPENDENT CLAIMS (37 CFR 1.16(h))	21 minus 3 =	18
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).	
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))		

RATE (\$)	FEE (\$)
N/A	150.00
N/A	\$250
N/A	\$100
X\$ 25 =	
X100 =	
+180=	
TOTAL	

RATE (\$)	FEE (\$)
N/A	300.00
N/A	\$500
N/A	\$200
X\$50 =	2750
X200 =	3600
+360=	
TOTAL	7350

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

APPLICATION AS AMENDED - PART II

(Column 1)

(Column 2)

(Column 3)

SMALL ENTITY

OR

OTHER THAN
SMALL ENTITY

AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total (37 CFR 1.16(i))	*	Minus	**	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=
	Application Size Fee (37 CFR 1.16(s))				
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					

RATE (\$)	ADDITIONAL FEE (\$)
X\$ 25 =	
X100 =	
+180=	
TOTAL ADD'L FEE	

RATE (\$)	ADDITIONAL FEE (\$)
X\$50 =	
X200 =	
+360=	
TOTAL ADD'L FEE	

AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total (37 CFR 1.16(i))	*	Minus	**	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=
	Application Size Fee (37 CFR 1.16(s))				
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					

RATE (\$)	ADDITIONAL FEE (\$)
X\$ 25 =	
X100 =	
+180=	
TOTAL ADD'L FEE	

RATE (\$)	ADDITIONAL FEE (\$)
X\$50 =	
X200 =	
+360=	
TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

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

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1460, Alexandria, VA 22313-1450.

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

PATENT
ELG-P-9139US2

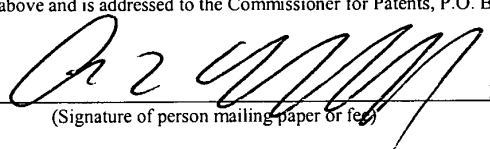
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants : Yigal Mordechai Edery et al.
U.S. Serial No. : unknown
Filed : herewith
Title : MALICIOUS MOBILE CODE RUNTIME MONITORING
SYSTEM AND METHODS
Group Art Unit : unknown
Examiner : unknown

EXPRESS MAIL MAILING LABEL NUMBER EO 399946563 US, Date of Deposit: March 7, 2006

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Andrew L. Tiajolloff
(Name of person mailing paper or fee)


(Signature of person mailing paper or fee)

March 7, 2006
Date

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRELIMINARY AMENDMENT

Sir:

Please amend the accompanying application as follows:

IN THE TITLE:

Please amend the Title as follows:

-- METHOD AND MALICIOUS MOBILE CODE RUNTIME MONITORING
SYSTEM FOR PROTECTING A COMPUTER AND METHODS A NETWORK
FROM HOSTILE DOWNLOADABLES

IN THE SPECIFICATION

On page 1, please amend the paragraph starting at line 5 as follows:

-- This application **is a continuation of assignee's pending application serial no. 09/861,229, filed on May 17, 2001, entitled "Malicious Mobile Code Runtime Monitoring System And Methods", which is hereby incorporated by reference.** **U.S. application serial no. 09/861,229** claims benefit of [~~and hereby incorporates by reference~~] provisional application serial number 60/205,591, entitled "Computer Network Malicious Code Run-time Monitoring," filed on May 17, 2000 by inventors Nimrod Itzhak Vered, et al., **which is hereby incorporated by reference. U.S. application serial no. 09/861,229** [~~This application~~] is also a Continuation-In-Part of [~~and hereby incorporates by reference~~] **U.S. patent application serial number 09/539,667, entitled "System and Method for Protecting a Computer and a Network From Hostile Downloadables" filed on March 30, 2000 by inventor Shlomo Touboul, now U.S. Patent 6,804,780, and hereby incorporated by reference, which is a continuation of assignee's patent application U.S. Serial No. 08/964,388, filed on November 6, 1997, now U.S. Patent No. 6,092,194, also entitled "System and Method for Protecting a Computer and a Network from Hostile Downloadables" and hereby incorporated by reference. U.S. Serial No. 09/861,229** [~~This application~~] is also a Continuation-In-Part of [~~and hereby incorporates by reference~~] U.S. patent application serial number 09/551,302, entitled "System and Method for Protecting a Client During Runtime From Hostile Downloadables", filed on April 18, 2000 by inventor Shlomo Touboul, **now U.S. Patent No. 6,480,962, which is hereby incorporated by reference.**

IN THE CLAIMS:

Please cancel the claims 1 to 76 without prejudice and add the following new claims:
1 to 76 (canceled).

77. (new) A computer-based method, comprising the steps of:
 receiving an incoming Downloadable;
 deriving security profile data for the Downloadable, including a list of
 suspicious computer operations that may be attempted by the Downloadable;
 and
 storing the Downloadable security profile data in a database.
78. (new) The computer-based method of claim 77 further comprising storing a date &
time when the Downloadable security profile data was derived in the database.
79. (new) The computer-based method of claim 77 wherein the Downloadable includes
a Java applet.
80. (new) The computer-based method of claim 77 wherein the Downloadable includes
an ActiveX control.
81. (new) The computer-based method of claim 77 wherein the Downloadable includes
a JavaScript script.
82. (new) The computer-based method of claim 77 wherein the Downloadable includes
a Visual Basic script.
83. (new) The computer-based method of claim 77 wherein suspicious computer
operations include calls made to an operating system, a file system, a network system, a
network system, and to memory.

84. (new) The computer-based method of claim 77 wherein the Downloadable security profile data includes a URL from where the Downloadable originated.
85. (new) The computer-based method of claim 77 wherein the Downloadable security profile data includes a digital certificate.
86. (new) The computer-based method of claim 77 wherein said deriving Downloadable security profile data comprises disassembling the incoming Downloadable.
87. (new) A system for managing Downloadables, comprising:
a receiver for receiving an incoming Downloadable;
a Downloadable scanner coupled with said receiver, for deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and
a database manager coupled with said Downloadable scanner, for storing the Downloadable security profile data in a database.
88. (new) The system of claim 87 wherein said database manager also stores a date & time when the Downloadable security profile data was derived by said Downloadable scanner, in the database.
89. (new) The system of claim 87 wherein the Downloadable includes a Java applet.
90. (new) The system of claim 87 wherein the Downloadable includes an ActiveX control.
91. (new) The system of claim 87 wherein the Downloadable includes a JavaScript script.
92. (new) The system of claim 87 wherein the Downloadable includes a Java applet.

93. (new) The system of claim 87 wherein suspicious computer operations include calls made to an operating system, a file system, a network system, and to memory.

94. (new) The system of claim 87 wherein the Downloadable security profile data includes a URL from where the Downloadable originated.

95. (new) The system of claim 87 wherein the Downloadable security profile data includes a digital certificate.

96. (new) The system of claim 87 wherein said Downloadable scanner comprises a disassembler for a disassembling the incoming Downloadable.

97. (new) A computer-based method, comprising the steps of:
receiving an incoming Downloadable;
deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable;
appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable; and
transmitting the appended Downloadable to a destination computer.

98. (new) The computer-based method of claim 97 wherein the Downloadable includes a Java applet.

99. (new) The computer-based method of claim 97 wherein the Downloadable includes an ActiveX control.

100. (new) The computer-based method of claim 97 wherein the Downloadable includes a JavaScript script.

101. (new) The computer-based method of claim 97 wherein the Downloadable includes a Visual Basic script.

102. (new) The computer-based method of claim 97 wherein suspicious computer operations include calls made to an operating system, a file system, a network system, and to memory.
103. (new) The computer-based method of claim 97 wherein the Downloadable security profile data includes a URL from where the Downloadable originated.
104. (new) The computer-based method of claim 97 wherein the appended Downloadable includes a digital certificate.
105. (new) The computer-based method of claim 97 wherein said deriving Downloadable security profile data comprises disassembling the incoming Downloadable.
106. (new) A system for managing Downloadables, comprising:
a receiver for receiving an incoming Downloadable;
a Downloadable scanner coupled with said receiver for deriving security profile data for Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable;
a file appender coupled with said Downloadable scanner, for appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended an appended Downloadable; and
a transmitter coupled with said file appender, for transmitting the appended Downloadable to a destination computer.
107. (new) The system of claim 106 wherein the Downloadable includes a Java applet.
108. (new) The system of claim 106 wherein the Downloadable includes a ActiveX control.
109. (new) The system of claim 106 wherein the Downloadable includes a JavaScript script.

110. (new) The system of claim 106 wherein the Downloadable includes a Visual Basic script.

111. (new) The system of claim 106 wherein suspicious computer operations include calls made to an operating system, a file system, a network system, and to memory.

112. (new) The system of claim 106 wherein the Downloadable security profile data includes a URL from where the Downloadable originated.

113. (new) The system of claim 106 wherein the appended Downloadable includes a digital certificate.

114. (new) The system of claim 106 wherein said Downloadable scanner comprises a disassembler for disassembling the incoming Downloadable.

115. (new) A computer-based method, comprising the steps of:
receiving an incoming Downloadable;
deriving security profile data for Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and
transmitting the Downloadable and a representation of the Downloadable security profile data to a destination computer, via a transport protocol transmission.

116. (new) The computer-based method of claim 115 wherein the transport protocol is an application transport protocol, and wherein the Downloadable security profile data is inserted as a header within the transport protocol transmission.

117. (new) The computer-based method of claim 116 wherein the application transport protocol is HTTP.

118. (new) The computer-based method of claim 116 wherein the application transport protocol is FTP.

119. (new) The computer-based method of claim 115 wherein the transport protocol is network transport protocol, and wherein the Downloadable security profile data is inserted as a frame within the transport protocol transmission.

120. (new) The computer-based method of claim 119 wherein the network transport protocol is TCP/IP.

121. (new) The computer-based method of claim 119 wherein the network transport protocol is UDP.

122. (new) A system for managing Downloadables, comprising:
a receiver for receiving an incoming Downloadable;
a Downloadable scanner coupled with said receiver, for deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and
a transmitter coupled with said receiver and with said Downloadable scanner, for transmitting the Downloadable and a representation of the Downloadable security profile data to a destination computer, via a transport protocol transmission.

123. (new) The system of claim 122 wherein the transport protocol is an application transport protocol and wherein the Downloadable security profile data is inserted as a header within the transport protocol transmission.

124. (new) The system of claim 123, wherein the application transport protocol is HTTP.

125. (new) The system of claim 123, wherein the application transport protocol is FTP.

126. (new) The system of claim 122 wherein the transport protocol is a network transport protocol, and wherein the Downloadable security profile data is inserted as a frame within the transport protocol transmission.

127. (new) The system of claim 126 wherein the network transport protocol is TCP/IP.

128. (new) The system of claim 126 wherein the network transport protocol is UDP.

129. (new) A computer-based method, comprising the steps of:
receiving an incoming Downloadable;
receiving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable;
appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable; and
transmitting the appended Downloadable to a destination computer.

130. (new) The computer-based method of claim 129 further comprising forwarding the Downloadable to an external computer, for deriving the Downloadable security profile data.

131. (new) A system for managing Downloadables, comprising:
a receiver for receiving an incoming Downloadable, and for receiving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable;
a file appender coupled with said receiver for appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable; and
a transmitter coupled with said file appender, for transmitting the appended Downloadable to a destination computer.

132. (new) The system of claim 131 wherein said transmitter forwards the Downloadable to an external computer, for deriving the Downloadable security profile data, and wherein said receiver receives the security profile data from the external computer.

133. (new) A computer-based method, comprising the steps of:
receiving an incoming Downloadable;
receiving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and
transmitting the Downloadable and a representation of the Downloadable security profile data to a destination computer, via a transport protocol transmission.

134. (new) The computer-based method of claim 133 further comprising forwarding the Downloadable to an external computer, for deriving the Downloadable security profile data.

135. (new) A system for managing Downloadables, comprising:
a receiver for receiving an incoming Downloadable, and for receiving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and
a transmitter coupled with said receiver, for transmitting the Downloadable and a representation of the Downloadable security profile data to a destination computer, via a transport protocol transmission.

136. (new) The system of claim 135 wherein said transmitter forwards the Downloadable to an external computer, for deriving the Downloadable security profile data, and wherein said receiver receives the security profile data from the external computer.

137. (new) A computer-based method, comprising the steps of:
receiving an incoming Downloadable addressed;
retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on an ID of the incoming Downloadable, the security profile data including a list of suspicious computer

operations that may be attempted by the Downloadable;

appending a representation of the retrieved Downloadable security profile data to the incoming Downloadable, to generate an appended Downloadable; and

transmitting the appended Downloadable to a destination computer.

138. (new) The computer-based method of claim 137 further comprising performing a hashing function on the incoming Downloadable to compute the incoming Downloadable ID.

139. (new) A system for managing Downloadables, comprising:

a receiver for receiving an incoming Downloadable addressed to a client;

a database manager for retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on an ID of the incoming Downloadable, the security profile data including a list of suspicious computer operations that may be attempted by the Downloadable;

a file appender coupled with said receiver for appending a representation of the Downloadable security profile data to the incoming Downloadable, to generate an appended Downloadable; and

a transmitter coupled with said file appender, for transmitting the appended Downloadable to a destination computer.

140. (new) The system of claim 139 further comprising a Downloadable identifier for performing a hashing function on the incoming Downloadable to compute the incoming Downloadable to compute the incoming Downloadable ID.

141. (new) A computer-based method, comprising the steps of:

receiving an incoming Downloadable;

receiving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on an ID of the incoming Downloadable, the security profile data including a list of suspicious computer operations that may be attempted by the Downloadable; and

transmitting the incoming Downloadable and a representation of the retrieved Downloadable security profiled data to a destination computer, via a transport protocol transmission.

142. (new) The computer-based method of claim 141 further comprising performing a hashing function on the incoming Downloadable to compute the incoming Downloadable ID.

143. (new) A system for managing Downloadable, comprising;
a receiver for receiving an incoming Downloadable addressed to a client;
a database manager for retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on an ID of the incoming Downloadable, the security profiled data including a list of suspicious computer operations that may be attempted by the Downloadable; and
a transmitter coupled with said receiver, for transmitting the incoming Downloadable and a representation of the retrieved Downloadable security profile data to a destination computer, via a transport protocol transmission.

144. (new) The system of claim 143 further comprising a Downloadable identifier for performing a hashing function on the incoming Downloadable to compute the incoming Downloadable to compute the incoming Downloadable ID.

145. (new) The system of claim 143 further comprising a Downloadable identifier for performing a hashing function on the incoming Downloadable to compute the incoming Downloadable ID.

receive an incoming Downloadable;
derive security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and
store the Downloadable security profile data in a database.

146. (new) A computer-readable storage medium storing program code for causing at least one computing device to:

- receive an incoming Downloadable;
- derive security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable;
- append a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable; and
- transmit the appended Downloadable to a destination computer.

147. (new) A computer-readable storage medium storing program code for causing at least one computing device to:

- receive an incoming Downloadable;
- derive security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and
- transmit the Downloadable and a representation of the Downloadable security profile data to a destination computer, via a transport protocol transmission.

148. (new) A computer-readable storage medium storing program code for causing at least one computing device to:

- receive an incoming Downloadable;
- receive security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable;
- append a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable; and
- transmit the appended Downloadable to a destination computer.

149. (new) A computer-readable storage medium storing program code for causing at least one computing device to:

- receive an incoming Downloadable;
- receive security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and

transmit the Downloadable and a representation of the Downloadable security profile data to a destination computer, via a transport protocol transmission.

150. (new) A computer-readable storage medium storing program code for causing at least one computing device to:

- receive an incoming Downloadable;
- retrieve security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on an ID of the incoming Downloadable, the security profiled data including a list of suspicious computer operations that may be attempted by the Downloadable;
- append a representation of the retrieved Downloadable security profile data to the incoming Downloadable, to generate an appended Downloadable; and
- transmit the appended Downloadable to a destination computer.

151. (new) A computer-readable storage medium storing program code for causing at least one computing device to:

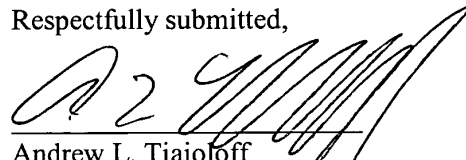
- receive an incoming Downloadable;
- retrieve security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on an ID of the incoming Downloadable, the security profiled data including a list of suspicious computer operations that may be attempted by the Downloadable; and
- transmit the incoming Downloadable and a representation of the retrieved Downloadable security profile data to a destination computer, via a transport protocol transmission.

REMARKS

This amendment inserts the assertion of US domestic priority for this application, amends the title, and adds new claims for the continuation.

Should any questions arise, the Patent Office is invited to telephone attorney for applicants at 212-490-3285.

Respectfully submitted,


A handwritten signature in black ink, appearing to read 'A L Tiajloff', is written over a horizontal line.

Andrew L. Tiajloff
Registration No. 31,575

Tiajloff & Kelly
Chrysler Building, 37th floor
405 Lexington Avenue
New York, NY 10174

tel. 212-490-3285
fax 212-490-3295

Application Data Sheet

Application Information

Application Type::	Regular
Subject Matter::	Utility
CD-ROM or CD-R?	None
Title::	METHOD AND SYSTEM FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES
Attorney Docket Number::	ELG-P-9139US2
Request for Early Publication?::	No
Request for Non-Publication?::	No
Suggested Drawing Figure::	3
Total Drawing Sheets::	10
Small Entity::	No
Petition included?::	No
Secrecy Order in Parent Appl.?::	No

Applicant Information

Applicant Authority type::	Inventor
Primary Citizenship Country:	Israel
Status::	Full Capacity
Given Name::	Yigal Mordechai
Family Name::	Edery
City::	Pardesia
Country:	Israel
Postal or Zip Code::	42815
Citizenship Country::	Israel

Applicant Authority type::	Inventor
Primary Citizenship Country:	Israel
Status::	Full Capacity

Given Name:: Nimrod Itzhak
Family Name:: Vered
City:: Goosh Tel-Mond
Country: Israel
Postal or Zip Code:: 40695
Citizenship Country:: Israel

Applicant Authority type:: Inventor
Primary Citizenship Country: USA
Status:: Full Capacity
Given Name:: David R.
Family Name:: Kroll
City:: San Jose
State:: California
Country: USA
Postal or Zip Code:: 96134
Citizenship Country:: USA

Applicant Authority type:: Inventor
Primary Citizenship Country: Israel
Status:: Full Capacity
Given Name:: Shlomo
Family Name:: Touboul
City:: Kefar-Haim
Country: Israel
Postal or Zip Code:: 42945
Citizenship Country:: Israel

Correspondence Information

Correspondence customer number:: 43214

Representative Information

Representative Designation::	Registration number::	Name::
Primary	31575	Andrew L. Tiajolloff
Associate	43116	Vladimir Sherman

Domestic Priority Information

Application::	Continuity Type:	Parent Application::	Parent Filing Date::
This Application	<i>Continuation of</i>	09/861,229	05/17/2001
09/861,229	<i>An application claiming the benefit under 35 USC 119(e)</i>	60/205,591	05/17/2000
09/861,229	<i>Continuation-in-part of</i>	09/551,302	04/18/2000
09/861,229	<i>Continuation-in-part of</i>	09/539,667	03/30/2000
09/539,667	<i>Continuation of</i>	08/964,388	11/06/1997

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 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	Unassigned
Filing Date	Unassigned
First Named Inventor	Yigal Edery
Art Unit	Unassigned
Examiner Name	Unassigned
Attorney Docket Number	ELG-P-9139-US2

Sheet	1	of	1
-------	---	----	---

U. S. PATENT DOCUMENTS

[illegible]

FOREIGN PATENT DOCUMENTS

[illegible]

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 Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. 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 here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

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

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875 Effective December 8, 2004

Application or Docket Number

11310114

APPLICATION AS FILED - PART I

(Column 1)

(Column 2)

SMALL ENTITY

OR

OTHER THAN SMALL ENTITY

FOR	NUMBER FILED	NUMBER EXTRA
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A
SEARCH FEE (37 CFR 1.16(d), (e), or (f))	N/A	N/A
EXAMINATION FEE (37 CFR 1.16(g), (h), or (i))	N/A	N/A
TOTAL CLAIMS (37 CFR 1.16(j))	75 minus 20 =	55
INDEPENDENT CLAIMS (37 CFR 1.16(k))	21 minus 3 =	18
APPLICATION SIZE FEE (37 CFR 1.16(l))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).	

MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))

RATE (\$)	FEE (\$)
N/A	150.00
N/A	\$250
N/A	\$100
X\$ 25 =	
X100 =	
+180=	
TOTAL	

RATE (\$)	FEE (\$)
N/A	300.00
N/A	\$500
N/A	\$200
X\$50 =	2750
X200 =	3600
+360=	
TOTAL	7350

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

APPLICATION AS AMENDED - PART II

AMENDMENT A	(Column 1)	(Column 2)	(Column 3)
	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total (37 CFR 1.16(j))	75	20	55
Independent (37 CFR 1.16(k))	20	3	17
Application Size Fee (37 CFR 1.16(s))			
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))			

RATE (\$)	ADDITIONAL FEE (\$)
X\$ 25 =	
X100 =	
+180=	
TOTAL ADD'L FEE	

RATE (\$)	ADDITIONAL FEE (\$)
X\$50 =	0
X200 =	0
+360=	
TOTAL ADD'L FEE	0

AMENDMENT B	(Column 1)	(Column 2)	(Column 3)
	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total (37 CFR 1.16(j))			
Independent (37 CFR 1.16(k))			
Application Size Fee (37 CFR 1.16(s))			
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))			

RATE (\$)	ADDITIONAL FEE (\$)
X\$ 25 =	
X100 =	
+180=	
TOTAL ADD'L FEE	

RATE (\$)	ADDITIONAL FEE (\$)
X\$50 =	
X200 =	
+360=	
TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

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

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

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

FACSIMILE COVER SHEET

CONFIDENTIAL AND PRIVILEGED

RECEIVED
CENTRAL FAX CENTER

JUN 16 2006

Perkins
Coie

If there are any problems with this transmission, please call:

☐ *Sender's name and phone number101 Jefferson Drive
Menlo Park, CA 94025-1114
PHONE: 650.838.4300
FAX: 650.838.4350
www.perkinscoie.comDATE: June 16, 2006 COVER SHEET & 3 PAGE(S)CLIENT NUMBER: 60644-8001.US03RETURN TO: (NAME) Sherry Castro (EXT.) 4310 (ROOM NO.) Menlo Park, CAORIGINAL DOCUMENT(S) WILL BE: ☐ SENT TO YOU ☒ HELD IN OUR FILES

SENDER:	TELEPHONE:	FACSIMILE:
Glenn E. Von Tersch, Reg. No. 41,364	(650) 838-4300	(650) 838-4350

RECIPIENT:	TELEPHONE:	FACSIMILE:
USPTO	N/A	(571) 273-8300

Please see the attached Forms. Thank you.

In re Application of EDERY et al.

Application No.: 11/370,114

Filed: March 7, 2006

For: Malicious Mobile Code Runtime Monitoring System and Methods

CERTIFICATE OF FACSIMILE TRANSMISSION (37 CFR 1.8a)

I hereby certify that this correspondence is being transmitted to the United States Patent & Trademark Office, Central Fax Service Center via facsimile number (571) 273-8300 on June 16, 2006.Date: June 16, 2006By: SCastro

Sherry Castro

This Fax contains confidential, privileged information intended only for the intended addressee. Do not read, copy or disseminate it unless you are the intended addressee. If you have received this Fax in error, please email it back to the sender at perkinscoie.com and delete it from your system or call us (collect) immediately at 650.838.4300, and mail the original Fax to Perkins Coie LLP, 101 Jefferson Drive, Menlo Park, CA 94025-1114.

ANCHORAGE • BEIJING • BELLEVUE • BOISE • CHICAGO • DENVER • HONG KONG • LOS ANGELES
MENLO PARK • OLYMPIA • PORTLAND • SAN FRANCISCO • SEATTLE • SPOKANE • WASHINGTON, D.C.
Perkins Coie LLP (Perkins Coie LLC in Illinois)

JUN 16 2006

PTO/SB/98 (05-04)

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.

STATEMENT UNDER 37 CFR 3.73(b)Applicant: Yigal M. Edery et al.Application No./Patent No.: 11/370,114 Filed/Issue Date: March 7, 2006Entitled: Malicious Mobile Code Runtime Monitoring System and MethodsFinjan Software, Ltd., a corporation
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☐ the assignee of the engine right, title, and interest; or
2. ☐ an assignee of less than the entire right, title and interest.
The extent (by percentage) of its ownership interest is _____ % in the patent application/patent identified above by virtue of either:
- A. ☐ An assignment from the inventor(s) of the parent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

OR

- B. ☒ A chain of title from the inventor(s), of the parent application/patent identified above, to the current assignee as shown below:

1. From: Yigal M. Edery, Nimrod I. Vered, David R. Kroll To: Finjan Software, Ltd.
The document was recorded in the United States Patent and Trademark Office at Reel 012748, Frame 0843, or for which a copy thereof is attached.
2. From: Shlomo Touboul To: Finjan Software, Ltd.
The document was recorded in the United States Patent and Trademark Office at Reel 016830, Frame 0387, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet.

☐ Copies of assignments or other documents in the chain of title are attached.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, if the assignment is to be recorded in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

June 16, 2006

Date

650-838-4328

Telephone number

Glenn E. Von Tersch

Typed or printed name

Glenn E. Von Tersch

Signature

Authorized Practitioner

Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-8199 and select option 2.

JUN 16 2006

Attorney Docket No. 60644-8001.US03

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

in re Application of: EDERY et al.
Application No.: 11/370,114
Filed: March 7, 2006
For: Malicious Mobile Code Runtime
Monitoring System and Methods

Examiner: Not Yet Assigned
Art Unit: Unknown
Conf. No: Unknown
Attorney Docket No.:
60644-8001.US03

Change of Address

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450


Sir:

Effective immediately, please direct all further communications in the above-identified patent to the following address, which is associated with Customer No. 22918:

**Glenn E. Von Tersch
Perkins Coie LLP
P. O. Box 2168
Menlo Park, CA 95026-2168**

Respectfully submitted,
Perkins Coie LLP

Date: June 16, 2006


Glenn E. Von Tersch
Registration No. 41,364

Correspondence Address:

Customer No. 22918
Perkins Coie LLP
P. O. Box 2168
Menlo Park, California 94026-2168
(650) 838-4300

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

in re Application of: EDERY et al.

Application No.: 11/370,114

Filed: March 7, 2006

For: Method and system for protecting a
computer and a network from hostile
downloadables

Examiner: Not Yet Assigned

Art Unit: 2131

Conf. No: 1442

Attorney Docket No.:
60644-8001.US03

Change of Address

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Effective immediately, please direct all further communications in the above-identified patent to the following address, which is associated with Customer No. 22918:

**Glenn E. Von Tersch
Perkins Coie LLP
P. O. Box 2168
Menlo Park, CA 95026-2168**

Respectfully submitted,
Perkins Coie LLP

Date: September 15, 2006

/Glenn E. Von Tersch/
Glenn E. Von Tersch
Registration No. 41,364

Correspondence Address:

Customer No. 22918
Perkins Coie LLP
P. O. Box 2168
Menlo Park, California 94026-2168
(650) 838-4300

STATEMENT UNDER 37 CFR 3.73(b)

Applicant: Yigal M. Edery et al.

Application No./Patent No.: 11/370,114 Filed/Issue Date: March 7, 2006

Entitled: Method and system for protecting a computer and a network from hostile downloadables

Finjan Software, Ltd., a corporation
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☐ the assignee of the engine right, title, and interest; or
2. ☐ an assignee of less than the entire right, title and interest.
The extent (by percentage) of its ownership interest is _____% in the patent application/patent identified above by virtue of either:
- A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

OR

- B. ☒ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as shown below:

1. From: Yigal M. Edery, Nimrod I. Vered, David R. Kroll To: Finjan Software, Ltd.
The document was recorded in the United States Patent and Trademark Office at Reel 012748, Frame 0843, or for which a copy thereof is attached.
2. From: Shlomo Touboul To: Finjan Software, Ltd.
The document was recorded in the United States Patent and Trademark Office at Reel 016830, Frame 0387, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet.

- ☐ Copies of assignments or other documents in the chain of title are attached.
[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, if the assignment is to be recorded in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

September 15, 2006
Date

Glenn E. Von Tersch
Typed or printed name

650-838-4328
Telephone number

/Glenn E. Von Tersch/
Signature

Authorized Practitioner
Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

PTO/SB/80 (12-03)

Approved for use through 11/30/2005. OMB 0651-0035

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.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby appoint

☒ Practitioners associated with the Customer Number: **22918**

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

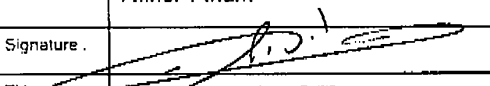
Assignee Name and Address:

Finjan Software, Ltd.
Shoham House
1 Hamachshev Street
New Industrial Area
Netanya 42504, ISRAEL

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Name	Asher Polani		
Signature		Date	20 March 06
Title	Chief Executive Officer	Telephone	011-972-9-864-8200

This collection of information is required by 37 CFR 1.31 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. 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.

[RV060760 089]

TOTAL P.02

Electronic Acknowledgement Receipt

EFS ID:	1204540
Application Number:	11370114
Confirmation Number:	1442
Title of Invention:	Method and system for protecting a computer and a network from hostile downloadables
First Named Inventor:	Yigal Mordechai Edery
Customer Number:	43214
Filer:	Glenn E. Von Tersch
Filer Authorized By:	
Attorney Docket Number:	ELG-P-9139US2
Receipt Date:	15-SEP-2006
Filing Date:	07-MAR-2006
Time Stamp:	22:35:18
Application Type:	Utility
International Application Number:	

Payment information:

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages
1	Change of Address	60644_8001US03_Change_Address.pdf	68925	no	1

Warnings:					
Information:					
2	Assignee showing of ownership per 37 CFR 3.73(b).	60644_8001US03_373_Statement.pdf	98321	no	1
Warnings:					
Information:					
3	Power of Attorney	60644_POA.pdf	48013	no	1
Warnings:					
Information:					
Total Files Size (in bytes):			215259		
<p>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.</p> <p><u>New Applications Under 35 U.S.C. 111</u> 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.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> 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.</p>					

RECEIVED
CENTRAL FAX CENTER**JUL 05 2007**

PTO/SO/M3 (01-05)

Approved for use through 12/31/2008, OMB 0851-0035

U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1996, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**REQUEST FOR WITHDRAWAL
AS ATTORNEY OR AGENT
AND CHANGE OF
CORRESPONDENCE ADDRESS**

Application Number	11/370,114
Filing Date	03-07-2006
First Named Inventor	Yigal Mordochai Edery
Art Unit	
Examiner Name	
Attorney Docket Number	ELG-P-0139US2

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

Please withdraw me as attorney or agent for the above identified patent application, and

- ☐ all the attorneys/agents of record.
- ☐ the attorneys/agents (with registration numbers) listed on the attached paper(s), or
- ☐ the attorneys/agents associated with Customer Number

NOTE: This box can only be checked when the power of attorney of record in the application is to all the practitioners associated with a customer number.

The reasons for this request are:

Instructed to withdraw by client

CORRESPONDENCE ADDRESS

1. ☐ The correspondence address is NOT affected by this withdrawal.
2. ☒ Change the correspondence address and direct all future correspondence to:

- ☒ The address associated with Customer Number:

OR☐ Firm or Individual Name

Address

City

State

Zip

Country

Telephone

Email

Signature

Name

Andrew L. Tiojolloff

Registration No.

31573

Date

7/5/07

Telephone No.

(212) 480-3285

NOTE: Withdrawal is effective when approved rather than when received. Unless there are at least 30 days between approval of withdrawal and the expiration date of a time period for response or possible extension period, the request to withdraw is normally disapproved.

This collection of information is required by 37 CFR 1.36. The information is required to obtain or retain a benefit by the public which is in file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

EMPK & SHILOH, LLP
116 JOHN STREET, SUITE 1201
NEW YORK, NY 10038

COPY MAILED

FEB 04 2008

In re Application of

EDERY, et al.

Application No. 11/370,114

Filed: March 7, 2006

Attorney Docket No. **60644-8001.US03**

:
:
:
:
:
:

OFFICE OF PETITIONS

**DECISION ON PETITION
TO WITHDRAW
FROM RECORD**

This is a decision on the Request to Withdraw as attorney or agent under 37 C.F.R. § 1.36(b) or 37 C.F.R. § 10.40 filed July 5, 2007.

The request is **NOT APPROVED**.

A review of the file record indicates that Andrew Tiajloff of **EMPK & SHILOH, LLP** does not have power of attorney in this patent application nor is there any statement or evidence of record of employment in or otherwise being engaged in the proceedings in this patent application. Accordingly, the request to withdraw under 37 C.F.R. § 1.36(b) is not applicable.

All future communications from the Office will continue to be directed to the below-listed address until otherwise properly notified by the applicant.

Telephone inquiries concerning this decision should be directed to the undersigned at (571) 272-7253.

Monica A. Graves
Petitions Examiner
Office of Petitions

CC: **PERKINS COIE, LLP
P.O. BOX 2168
MENLO PARK, CA 94026**

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:



Practitioners associated with the Customer Number:

74877

OR



Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:



The address associated with Customer Number:

74877

OR

<input type="checkbox"/> Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone			Email

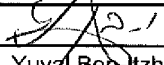
Assignee Name and Address:

Finjan Software
Shoham House, 1 Hamachshev Street
New Industrial Area, Netangy 42504 ISRAEL

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	Oct 30 th 2008
Name	Yuval Ben-Itzhak	Telephone	+ 972 (9) 864 8243
Title	Chief Technology Officer, Finjan Software		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Eder Yigal, et al.

Application No./Patent No.: 11/370,114

Filed/Issue Date: March 7, 2006

Entitled: Method and system for protecting a computer and a network from hostile downloadables

FINJAN SOFTWARE, LTD.

, a corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☒ the assignee of the entire right, title, and interest; or
2. ☐ an assignee of less than the entire right, title, and interest

The extent (by percentage) of its ownership interest is _____ %

in the patent application/patent identified above by virtue of either:

- A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 012748 and 016830, Frame 0843 and 0387, respectively, or for which a copy thereof is attached.

OR

- B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as shown below:

1. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

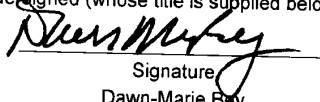
3. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet.

☐ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE:] A separate copy (i.e., a true copy of the original document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, if the assignment is to be recorded in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.


Signature

Dawn-Marie Bey

Printed or Typed Name

Partner, King & Spalding LLP

Title

10-31-08

Date

202 737 0500

Telephone Number

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

Electronic Acknowledgement Receipt	
EFS ID:	4213789
Application Number:	11370114
International Application Number:	
Confirmation Number:	1442
Title of Invention:	Method and system for protecting a computer and a network from hostile downloadables
First Named Inventor/Applicant Name:	Yigal Mordechai Edery
Customer Number:	22918
Filer:	Dawn-Marie Bey./Terry Goad
Filer Authorized By:	Dawn-Marie Bey.
Attorney Docket Number:	60644-8001.US03
Receipt Date:	31-OCT-2008
Filing Date:	07-MAR-2006
Time Stamp:	14:40:43
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	Power of Attorney	FinjanPOA.pdf	156559 0c8c2be8d4dbddb705c9cac8796e35fd80a6ecc	no	1

Warnings:

Information:

2	Assignee showing of ownership per 37 CFR 3.73(b).	11-370114.pdf	60402 32aaeb9c2fcad717479ca907005d240cfe4a269	no	1
Warnings:					
Information:					
Total Files Size (in bytes):				216961	
<p>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.</p> <p><u>New Applications Under 35 U.S.C. 111</u> 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.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> 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.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> 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.</p>					



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/370,114	03/07/2006	Yigal Mordechai Edery	60644-8001.US03

CONFIRMATION NO. 1442

POA ACCEPTANCE LETTER

74877

King and Spalding LLP
1700 Pennsylvania Ave, NW
Suite 200
Washington, DC 20006



Date Mailed: 11/12/2008

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/31/2008.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/snguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/370,114	03/07/2006	Yigal Mordechai Edery	60644-8001.US03

CONFIRMATION NO. 1442

POWER OF ATTORNEY NOTICE

22918
PERKINS COIE LLP
P.O. BOX 1208
SEATTLE, WA 98111-1208



Date Mailed: 11/12/2008

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/31/2008.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/snguyen/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/370,114	03/07/2006	Yigal Mordechai Edery	FIN0001-CON1-CIP1-CON2	1442
74877 7590 02/25/2009 King and Spalding LLP 1700 Pennsylvania Ave, NW Suite 200 Washington, DC 20006			EXAMINER REVAK, CHRISTOPHER A	
			ART UNIT 2431	PAPER NUMBER
			MAIL DATE 02/25/2009	DELIVERY MODE PAPER

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

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

Office Action Summary	Application No. 11/370,114		Applicant(s) EDERY ET AL.	
	Examiner Christopher A. Revak		Art Unit 2431	

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

Period for Reply

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

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

Status

1) ☒ Responsive to communication(s) filed on 07 March 2006.

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) 77-151 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) 77-151 is/are rejected.

7) ☐ Claim(s) 138, 140, 142, 144 and 145 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 07 March 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) ☐ All b) ☐ Some * c) ☐ None of:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. _____.

3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date <u>3/7/06</u> .	4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____. 5) <input type="checkbox"/> Notice of Informal Patent Application 6) <input type="checkbox"/> Other: _____.
--	--

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on June 22, 2005 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

2. The disclosure is objected to because of the following informalities:

On page 1, beginning at line 5, reference is made to application 09/861,229 which is now U.S. Patent 7,058,822

Appropriate correction is required.

Double Patenting

3. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re 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(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to

be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

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).

4. Claims 77-151 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-68 of U.S. Patent No. 6,092,194. Although the conflicting claims are not identical, they are not patentably distinct from each other because the claims of the instant application are anticipated by patent claims 1-68 such the claims of the patent contain all the limitations of the instant application. Claims 77-151 of the instant application therefore are not patentably distinct from the earlier patent claims, and as such, is unpatentable under obvious-type double patenting.
5. Claims 77-151 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-44 of U.S. Patent No. 6,154,844. Although the conflicting claims are not identical, they are not patentably distinct from each other because the claims of the instant application are anticipated by patent claims 1-44 such the claims of the patent contain all the limitations of the instant application. Claims 77-151 of the instant application therefore are not patentably distinct from the earlier patent claims, and as such, is unpatentable under obvious-type double patenting.
6. Claims 77-151 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-18 of U.S. Patent No. 6,154,844. Although the conflicting claims are not identical, they are not patentably distinct from each other because the claims of the instant application are anticipated by patent claims 1-18 such the claims of the patent contain all the limitations of the instant application.

Claims 77-151 of the instant application therefore are not patentably distinct from the earlier patent claims, and as such, is unpatentable under obvious-type double patenting

Claim Rejections - 35 USC § 112

7. 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.

8. Claims 79-82,89-92,98-101, and 107-110 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The Claims contains the trademark/trade name Java™, ActiveX™, JavaScript™, Visual Basic™. 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 software executables and, accordingly, the identification/description is indefinite.

Claim Rejections - 35 USC § 102

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

A person shall be entitled to a patent unless –

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

10. Claims 77,79-83,86,87,89-93,96-102,105-11,114-137,139,141,143, and 146-151 are rejected under 35 U.S.C. 102(e) as being anticipated by Ji, U.S. Patent 5,983,348.

As per claims 77,87,97,106, and 146, it is taught of a computer-based method, comprising the steps of receiving an incoming Downloadable; deriving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and storing the Downloadable security profile data in a database (col. 3, lines 16-56; col. 4, line 66 through col. 5, line 27; and col. 6, lines 39-51).

As per claims 79,89,98, and 107, it is taught wherein the Downloadable includes a Java applet (col. 3, lines 16-23).

As per claims 80,90,99, and 108, it is disclosed wherein the Downloadable includes an ActiveX control (col. 3, lines 16-23).

As per claims 81,91,100, and 109, it is taught wherein the Downloadable includes a JavaScript script (col. 3, lines 16-23).

As per claims 82,92,101, and 110, it is disclosed wherein the Downloadable includes a Visual Basic script (col. 3, lines 16-23).

As per claims 83,93,102, and 111, it is taught wherein suspicious computer operations include calls made to

an operating system, a file system, a network system, a network system, and to memory (col. 5, lines 16-27).

As per claims 86,96,105, and 114, it is disclosed wherein said deriving Downloadable security profile data comprises disassembling the incoming Downloadable (col. 4, line 66 through col. 5, line 27).

As per claims 115,122,147, and 149, it is disclosed of a computer-based method, comprising the steps of receiving an incoming Downloadable; deriving security profile data for Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; and transmitting the Downloadable and a representation of the Downloadable security profile data to a destination computer, via a transport protocol transmission (col. 3, lines 16-56; col. 4, line 66 through col. 5, line 27; and col. 6, lines 39-51).

As per claims 116 and 123, it is taught wherein the transport protocol is an application transport protocol, and wherein the Downloadable security profile data is inserted as a header within the transport protocol transmission (col. 3, lines 7-9 & 16-23 and col. 5, lines 16-27).

As per claims 117 and 124, it is disclosed wherein the application transport protocol is HTTP (col. 3, lines 7-9 & 16-23).

As per claims 118 and 125, it is taught wherein the application transport protocol is FTP (col. 3, lines 7-9 & 16-23).

As per claims 119 and 126, it is disclosed wherein the transport protocol is network transport protocol, and wherein the Downloadable security profile data is inserted as a frame within the transport protocol transmission (col. 3, lines 7-9 & 16-23 and col. 5, lines 16-27).

As per claims 120 and 127, it is taught wherein the network transport protocol is TCP/IP (col. 3, lines 7-9 & 16-23).

As per claims 121 and 128, it is disclosed wherein the network transport protocol is UDP (col. 3, lines 7-9 & 16-23).

As per claims 129,131,133,135, and 148, it is disclosed of a computer-based method, comprising the steps of receiving an incoming Downloadable; receiving security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable; appending a representation of the Downloadable security profile data to the Downloadable, to generate an appended Downloadable; and transmitting the appended Downloadable to a destination computer (col. 3, lines 16-56; col. 4, line 66 through col. 5, line 27; and col. 6, lines 39-51).

As per claims 130, 132,134, and 136, it is taught of further comprising forwarding the Downloadable to an external computer, for deriving the Downloadable security profile data (col. 4, line 66 through col. 5, line 27).

As per claims 137,139,141,143,150, and 151, it is disclosed of a computer-based method, comprising the steps of receiving an incoming Downloadable addressed;

retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on an ID of the incoming Downloadable, the security profile data including a list of suspicious computer operations that may be attempted by the Downloadable; appending a representation of the retrieved Downloadable security profile data to the incoming Downloadable, to generate an appended Downloadable; and transmitting the appended Downloadable to a destination computer (col. 3, lines 16-56; col. 4, line 66 through col. 5, line 27; and col. 6, lines 39-51).

Claim Rejections - 35 USC § 103

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

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

12. Claims 78,84,85,88,94,95,103,104,112, and 113 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ji, U.S. Patent 5,983,348.

As per claims 78 and 88, Ji fails to teach of storing a date & time when the Downloadable security profile data was derived in the database. The examiner hereby takes official notice that it is notoriously well known to one of ordinary skill that date and time information is included whenever a file or created or modified in any sort. It is obvious to a person of ordinary skill at the time of the invention that by including date

and time information, it can be determined when any changes or modifications occurred to a file.

As per claims 84,94,103, and 112, Ji fails to disclose of including a URL from where the Downloadable originated. The examiner hereby takes official notice that files include URL information which indicates where the source of the file came from. It is obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to include URL information which indicates the source of executable content which can then be traced back to its particular source.

As per claims 85,95,104, and 113, Ji teaches of signing the content (col. 4, line 66 through col. 5, line 27), but fails to teach of including a digital certificate to certify content. The examiner hereby takes official notice that the use of a digital certificate to certify content is notoriously well known to one of ordinary skill in the art. 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 use digital certificates as a means of certifying the signed content. Digital certificates are notoriously well known as a means of providing that the content is from a trusted source which can be verified through the certificate authority. The teachings of Ji disclose of the use of signing the content and digital certificates are known to include digital signatures, it is obvious that the teachings of Ji would include the use of digital certificates to prove that the signed content is from a trusted source.

Allowable Subject Matter

13. Claims 138,140,142,144, and 145 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Thursday, 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571)272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

Application/Control Number: 11/370,114
Art Unit: 2431

Page 11

/Christopher A. Revak/
Primary Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 11/370,114	Applicant(s)/Patent Under Reexamination EDERY ET AL.	
	Examiner Christopher A. Revak	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,732,179	05-2004	Brown et al.	709/229
*	B	US-5,606,668	02-1997	Shwed, Gil	726/13
*	C	US-5,623,600	04-1997	Ji et al.	726/24
*	D	US-6,092,194	07-2000	Touboul, Shlomo	726/24
*	E	US-6,154,844	11-2000	Touboul et al.	726/24
*	F	US-7,058,822	06-2006	Edery et al.	726/22
*	G	US-6,480,962	11-2002	Touboul, Shlomo	726/22
*	H	US-6,804,780	10-2004	Touboul, Shlomo	713/181
	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	
	V	
	W	
	X	

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




UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 1442

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
11/370,114	03/07/2006	713	2431	FIN0001-CON1-CIP1-CON2		
APPLICANTS Yigal Mordechai Edery, Pardesia, ISRAEL; Nimrod Itzhak Vered, Goosh Tel-Mond, ISRAEL; David R. Kroll, San Jose, CA; Shlomo Touboul, Kefar-Haim, ISRAEL;						
** CONTINUING DATA ***** This application is a CIP of 09/861,229 05/17/2001 PAT 7,058,822 which claims benefit of 60/205,591 05/17/2000 and is a CIP of 09/539,667 03/30/2000 PAT 6,804,780 which is a CON of 08/964,388 11/06/1997 PAT 6,092,194 and said 09/861,229 05/17/2001 is a CIP of 09/551,302 04/18/2000 PAT 6,480,962						
** FOREIGN APPLICATIONS *****						
** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 03/30/2006						
Foreign Priority claimed <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No 35 USC 119(a-d) conditions met <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Verified and /CHRISTOPHER A Acknowledged REVAK/ Examiner's Signature		<input type="checkbox"/> Met after Allowance /CR/ Initials	STATE OR COUNTRY ISRAEL	SHEETS DRAWINGS 10	TOTAL CLAIMS 75	INDEPENDENT CLAIMS 21
ADDRESS King and Spalding LLP 1700 Pennsylvania Ave, NW Suite 200 Washington, DC 20006 UNITED STATES						
TITLE Method and system for protecting a computer and a network from hostile downloadables						
FILING FEE RECEIVED 7350	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit		


Search Notes 	Application/Control No. 11370114	Applicant(s)/Patent Under Reexamination EDERY ET AL.
	Examiner Christopher A Revak	Art Unit 2431

SEARCHED			
Class	Subclass	Date	Examiner
none	none	2/16/09	CR

SEARCH NOTES		
Search Notes	Date	Examiner
PALM Inventor Name Search	2/16/09	CR
BRS Text Search: USPAT, US PGPUB, USOCR, DERWENT, FPRS, IBM TDB, EPO, JPO (see attached search strategy)	2/16/09	CR
BRS Subclass Text Search: USPAT, US PGPUB (see attached search strategy)	2/16/09	CR


INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

<p><i>Index of Claims</i></p> 	Application/Control No. 11370114	Applicant(s)/Patent Under Reexamination EDERY ET AL.
	Examiner Christopher A Revak	Art Unit 2431


✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant <input type="checkbox"/> CPA <input type="checkbox"/> T.D. <input type="checkbox"/> R.1.47										
CLAIM		DATE								
Final	Original	02/16/2009								
	77	✓								
	78	✓								
	79	✓								
	80	✓								
	81	✓								
	82	✓								
	83	✓								
	84	✓								
	85	✓								
	86	✓								
	87	✓								
	88	✓								
	89	✓								
	90	✓								
	91	✓								
	92	✓								
	93	✓								
	94	✓								
	95	✓								
	96	✓								
	97	✓								
	98	✓								
	99	✓								
	100	✓								
	101	✓								
	102	✓								
	103	✓								
	104	✓								
	105	✓								
	106	✓								
	107	✓								
	108	✓								
	109	✓								
	110	✓								
	111	✓								
	112	✓								

<i>Index of Claims</i> 	Application/Control No. 11370114	Applicant(s)/Patent Under Reexamination EDERY ET AL.
	Examiner Christopher A Revak	Art Unit 2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant			<input type="checkbox"/> CPA			<input type="checkbox"/> T.D.			<input type="checkbox"/> R.1.47		
CLAIM		DATE									
Final	Original	02/16/2009									
	113	✓									
	114	✓									
	115	✓									
	116	✓									
	117	✓									
	118	✓									
	119	✓									
	120	✓									
	121	✓									
	122	✓									
	123	✓									
	124	✓									
	125	✓									
	126	✓									
	127	✓									
	128	✓									
	129	✓									
	130	✓									
	131	✓									
	132	✓									
	133	✓									
	134	✓									
	135	✓									
	136	✓									
	137	✓									
	138	O									
	139	✓									
	140	O									
	141	✓									
	142	O									
	143	✓									
	144	O									
	145	O									
	146	✓									
	147	✓									
	148	✓									

<p align="center"><i>Index of Claims</i></p> 	Application/Control No. 11370114	Applicant(s)/Patent Under Reexamination EDERY ET AL.
	Examiner Christopher A Revak	Art Unit 2431

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant <input type="checkbox"/> CPA <input type="checkbox"/> T.D. <input type="checkbox"/> R.1.47										
CLAIM		DATE								
Final	Original	02/16/2009								
	149	✓								
	150	✓								
	151	✓								

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	299268	(code or executable or download\$5 or applet or java or javascript or script or activex) with(determin\$5 or ascertain\$3 or monitor\$3 or analy\$4 or inspect\$3 or examin\$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/02/16 09:56
L2	471422	(code or executable or download\$5 or applet or java or javascript or script or activex) with(append\$3 or attach\$3 or indicat\$3 or profile or character\$5 or identif\$7 or report\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/02/16 09:57
L3	83415	1 with 2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/02/16 09:57
L4	458238	(transmi\$5 or send\$3 or sent or communicat\$3 or forward\$3)with (secure or environment or shell or sandbox or protect\$3 or quarantin\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/02/16 09:59
L5	18076	4 with(code or executable or download\$5 or applet or java or javascript or script or activex)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/02/16 09:59

L6	1659	1 with 5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/02/16 10:00
L7	518	3 same 6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/02/16 10:00
L8	2303	1 with(malicious or suspicious or attack or malware or virus or viral or intrusion or trojan or worm)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/02/16 10:02
L9	15	7 same 8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/02/16 10:02
L10	20	7 and 8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/02/16 10:02
L11	3193	(726/22-25).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/02/16 10:02
L12	17	7 and 11	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/02/16 10:02

2/16/09 10:04:33 AM

C:\Documents and Settings\crevak\My Documents\EAST\Workspaces\default1.wsp

PTO/SB/08A (07-05)

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 contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known

Application Number	Unassigned
Filing Date	Unassigned
First Named Inventor	Yigal Edery
Art Unit	Unassigned
Examiner Name	Unassigned
Attorney Docket Number	ELG-P-9139-US2

Sheet	1	of	1
-------	---	----	---

U. S. PATENT DOCUMENTS

[illegible]

FOREIGN PATENT DOCUMENTS

[illegible]

Examiner Signature	/Christopher Revak/	Date Considered	02/16/2009
--------------------	---------------------	-----------------	------------

*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 Applicant's unique citation designation number (optional).² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. 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 here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, 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 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /CR/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Patent Application of:)
)
Yigal Mordechai Edery) Examiner: Christopher A. Revak
Nimrod Itzhak Vered) Art Unit: 2431
David R. Kroll)
Shlomo Touboul)
)
Application No: 11/370,114)
)
Filed: March 7, 2006)
)
For: METHOD AND SYSTEM FOR)
PROTECTING A COMPUTER)
AND A NETWORK FROM)
HOSTILE DOWNLOADABLES)
_____)

FILED ELECTRONICALLY

Mail Stop AMENDMENT
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 February 25, 2009,
applicants respectfully request that the above-identified application be
amended as follows:

IN THE SPECIFICATION

Please replace the first paragraph on page 2 with the following:

This application is a continuation of assignee's pending application serial no. 09/861,229, filed on May 17, 2001, now U.S. patent number 7,058,822, entitled "Malicious Mobile Code Runtime Monitoring System And Methods", which is hereby incorporated by reference. U.S. application serial no. 09/861,229 claims benefit of provisional application serial number 60/205,591, entitled "Computer Network Malicious Code Run-time Monitoring," filed on May 17, 2000 by inventors Nimrod Itzhak Vered, et al., which is hereby incorporated by reference. U.S. application serial no. 09/861,229 is also a Continuation-In-Part of U.S. patent application serial number 09/539,667, entitled "System and Method for Protecting a Computer and a Network From Hostile Downloadables" filed on March 30, 2000 by inventor Shlomo Touboul, now U.S. Patent No. 6,804,780, and hereby incorporated by reference, which is a continuation of assignee's patent application U.S. Serial No. 08/964,388, filed on November 6, 1997, now U.S. Patent No. 6,092,194, also entitled "System and Method for Protecting a Computer and a Network from Hostile Downloadables" and hereby incorporated by reference. U.S. Serial No. 09/861,229 is also a Continuation-In-Part of U.S. patent application serial number 09/551,302, entitled "System and Method for Protecting a Client During Runtime From Hostile Downloadables", filed on April 18, 2000 by inventor Shlomo Touboul, now U.S. Patent No. 6,480,962, which is hereby incorporated by reference.

Please replace the paragraph on page 11, lines 3-4 with the following:

FIG. ~~7~~8 is a block diagram illustrating a mobile protection code according to an embodiment of the invention;

Please delete the paragraph on page 11, lines 5-6:

~~FIG. 8 is a flowchart illustrating a method for examining a Downloadable in accordance with the present invention;~~

Please replace the paragraph on page 11, lines 7-8 with the following:

FIG. 9 is a flowchart illustrating a ~~server-based~~ protection method according to an embodiment of the invention;

IN THE DRAWINGS

Please replace the original Figure 8, with the attached replacement sheet.

IN THE CLAIMS

Please cancel claims **77 – 136, 138, 140, 142 and 144 – 149** without prejudice.

Please substitute the following claims for the pending claims with the same number:

1. – 136. (canceled)

137. (currently amended) A computer-based method, comprising the steps of:

- receiving an incoming Downloadable ~~addressed~~;
- performing a hashing function on the incoming Downloadable to compute an incoming Downloadable ID;
- retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on ~~an ID~~ of the incoming Downloadable ID, the security profile data including a list of suspicious computer operations that may be attempted by the Downloadable;
- appending a representation of the retrieved Downloadable security profile data to the incoming Downloadable, to generate an appended Downloadable; and
- transmitting the appended Downloadable to a destination computer.

138. (canceled)

139. (currently amended) A system for managing Downloadables, comprising:

- a receiver for receiving an incoming Downloadable ~~addressed to a client;~~

- a Downloader identifier for performing a hashing function on the incoming Downloadable to compute an incoming Downloadable ID;

- a database manager for retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on ~~an ID~~ of the incoming Downloadable ID, the security ~~profiled~~ profile data including a list of suspicious computer operations that may be attempted by the Downloadable;

- a file appender coupled with said receiver for appending a representation of the Downloadable security profile data to the incoming Downloadable, to generate an appended Downloadable; and

- a transmitter coupled with said file appender, for transmitting the appended Downloadable to a destination computer.

140. (canceled)

141. (currently amended) A computer-based method, comprising the steps of:

- receiving an incoming Downloadable;

- performing a hashing function on the incoming Downloadable to compute an incoming Downloadable ID;

- retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to

Downloadable IDs, based on ~~an ID~~ of the incoming Downloadable ID, the security ~~profiled~~ profile data including a list of suspicious computer operations that may be attempted by the Downloadable; and

transmitting the incoming Downloadable and a representation of the retrieved Downloadable security ~~profiled~~ profile data to a destination computer, via a transport protocol transmission.

142. (canceled)

143. (currently amended) A system for managing ~~Downloadable~~ Downloadables, comprising:

a receiver for receiving an incoming Downloadable ~~addressed to a client~~;

a Downloadable identifier for performing a hashing function on the incoming Downloadable to compute an incoming Downloadable ID;

a database manager for retrieving security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on ~~an ID~~ of the incoming Downloadable ID, the security ~~profiled~~ profile data including a list of suspicious computer operations that may be attempted by the Downloadable; and

a transmitter coupled with said receiver, for transmitting the incoming Downloadable and a representation of the retrieved Downloadable security profile data to a destination computer, via a transport protocol transmission.

144. – 149. (canceled)

150. (currently amended) A computer-readable storage medium storing program code for causing at least one computing device to:

- receive an incoming Downloadable;
- perform a hashing function on the incoming Downloadable to compute an incoming Downloadable ID;
- retrieve security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on ~~an ID of~~ the incoming Downloadable ID, the security ~~profiled~~ profile data including a list of suspicious computer operations that may be attempted by the Downloadable;
- append a representation of the retrieved Downloadable security profile data to the incoming Downloadable, to generate an appended Downloadable; and
- transmit the appended Downloadable to a destination computer.

151. (currently amended) A computer-readable storage medium storing program code for causing at least one computing device to:

- receive an incoming Downloadable;
- perform a hashing function on the incoming Downloadable to compute an incoming Downloadable ID;
- retrieve security profile data for the incoming Downloadable from a database of Downloadable security profiles indexed according to Downloadable IDs, based on ~~an ID of~~ the incoming Downloadable ID, the security ~~profiled~~ profile data including a list of suspicious computer operations that may be attempted by the Downloadable; and

transmit the incoming Downloadable and a representation of the retrieved Downloadable security profile data to a destination computer, via a transport protocol transmission.

Please add the following new claims.

152. (new) The computer-based method of claim **137** wherein the Downloadable includes an applet.

153. (new) The computer-based method of claim **137** wherein the Downloadable includes an active control.

154. (new) The computer-based method of claim **137** wherein the Downloadable includes program script.

155. (new) The computer-based method of claim **137** wherein suspicious computer operations include calls made to an operating system, a file system, a network system, and to memory.

156. (new) The computer-based method of claim **137** wherein the Downloadable security profile data includes a URL from where the Downloadable originated.

157. (new) The computer-based method of claim **137** wherein the Downloadable security profile data includes a digital certificate.

158. (new) The system of claim **139** wherein the Downloadable includes an applet.

159. (new) The system of claim **139** wherein the Downloadable includes an active control.

160. (new) The system of claim **139** wherein the Downloadable includes program script.

161. (new) The system of claim **139** wherein suspicious computer operations include calls made to an operating system, a file system, a network system, and to memory.

162. (new) The system of claim **139** wherein the Downloadable security profile data includes a URL from where the Downloadable originated.

163. (new) The system of claim **139** wherein the Downloadable security profile data includes a digital certificate.

164. (new) The computer-based method of claim **141** wherein the Downloadable includes an applet.

165. (new) The computer-based method of claim **141** wherein the Downloadable includes an active control.

166. (new) The computer-based method of claim **141** wherein the Downloadable includes program script.

167. (new) The computer-based method of claim **141** wherein suspicious computer operations include calls made to an operating system, a file system, a network system, and to memory.

168. (new) The computer-based method of claim **141** wherein the Downloadable security profile data includes a URL from where the Downloadable originated.

169. (new) The computer-based method of claim **141** wherein the Downloadable security profile data includes a digital certificate.

170. (new) The system of claim **143** wherein the Downloadable includes an applet.

171. (new) The system of claim **143** wherein the Downloadable includes an active control.

172. (new) The system of claim **143** wherein the Downloadable includes program script.

173. (new) The system of claim **143** wherein suspicious computer operations include calls made to an operating system, a file system, a network system, and to memory.

174. (new) The system of claim **143** wherein the Downloadable security profile data includes a URL from where the Downloadable originated.

175. (new) The system of claim **143** wherein the Downloadable security profile data includes a digital certificate.

REMARKS

Applicants have 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.

Applicants have amended **FIG. 8** to correct an error; specifically, to renumber element **361** in **FIG. 8** as element **341**. The element was originally intended to be numbered **341**, as indicated at page 38, lines 8 and 12 of the original specification, and there is no mention of element **361** anywhere in the specification

Applicants have canceled claims **77 - 136, 138, 140, 142** and **144 - 149**, have amended claims **137, 139, 141, 143, 150** and **151**, and have added new claims **152 - 175** to more properly claim the present invention. No new matter has been introduced. Claims **137, 139, 141, 143** and **150 - 175** are presented for examination.

In Paragraph 1 of the Office Action, the Examiner has objected to the specification because an informality. Applicants have amended the specification accordingly.

In Paragraphs 2 - 6 of the Office Action, the Examiner has rejected claims **77 - 151** on the ground of non-statutory obviousness-type double patenting as being unpatentable over claims **1 - 68** of U.S. Patent No. 6,092,194, and over claims **1 - 44** of U.S. Patent No. 6,154,844. Applicants note that the Examiner referenced U.S. Patent No. 6,154,844 on both paragraphs 5 and 6. The undersigned representative believes that the Examiner intended to reference U.S. Patent No. 6,804,780 in paragraph 6.

Applicants are accordingly filing a terminal disclaimer concurrent with this response.

In Paragraph 13 of the Office Action, the Examiner has indicated that claims **138, 140, 142** and **144** would be allowable if rewritten in independent form including all limitations of the base claim and any intervening claims. Applicants have accordingly amended base independent claims **137, 139, 141** and **143** to incorporate the limitations of respective dependent claims **138, 140, 142** and **144**. Applicants have also amended base independent claims **150** and **151**, for a computer-readable storage medium, to incorporate the limitations of respective dependent claims **138** and **142**. Amended independent claims **150** and **151** are consistent with amended independent claims **137** and **141**.

Support for New and Amended Claims in Original Specification

Independent claims **137, 139, 141** and **143** have been amended to include the limitations of respective original dependent claims **138, 140, 142** and **144**. Independent claims **150** and **151** have been amended to include the limitations of respective original dependent claims **138** and **142**.

New dependent claims **152 – 157** correspond to original dependent claims **79 – 81** and **83 – 85**.

New dependent claims **158 – 163** correspond to original dependent claims **89 – 91** and **93 – 95**.

New dependent claims **164 – 169** correspond to original dependent claims **79 – 81** and **83 – 85**.

New dependent claims **170 – 175** correspond to original dependent claims **89 – 91** and **93 – 95**.

CONCLUSION

The undersigned representative respectfully submits that this application is in condition for allowance, and such disposition is earnestly solicited. If the Examiner believes that the prosecution might be advanced by discussing the application with the undersigned representative, in person or over the telephone, we welcome the opportunity to do so. In addition, if any additional fees are required in connection with the filing of this response, the Commissioner is hereby authorized to charge the same to Deposit Account 50-4402.

Respectfully submitted,

Date: May 26, 2009

By: /Eric Sophir, Reg. No. 48,499/

KING & SPALDING LLP
1700 Pennsylvania Ave., NW, Suite 200
Washington, DC 20006
(202) 626-8980

Eric L. Sophir
Registration No. 48,499

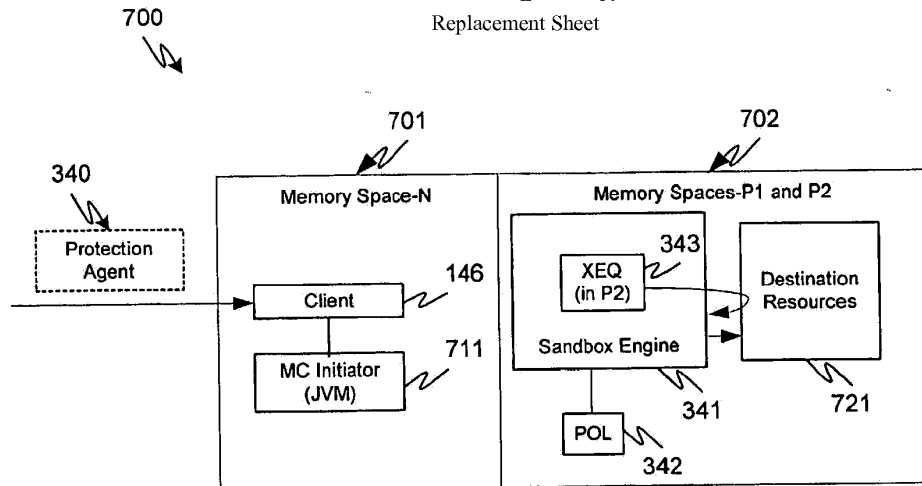


FIG. 7a

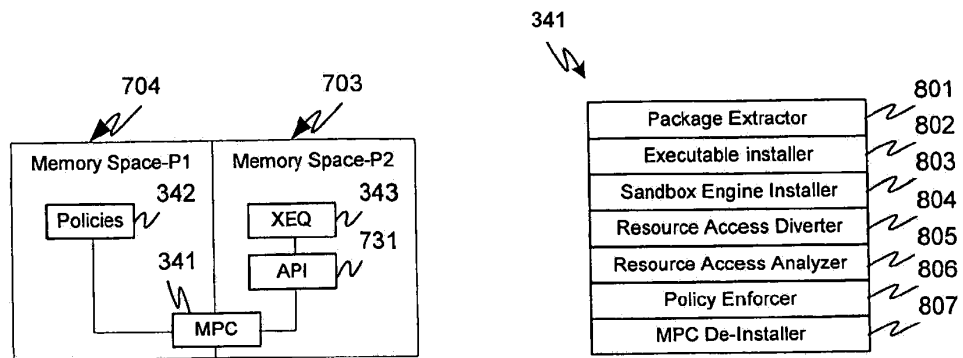


FIG. 7b

FIG. 8

**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING
REJECTION OVER A "PRIOR" PATENT**Docket Number (Optional)
FIN0001-CON1-CIP1-CON2

In re Application of: Yigal Mordechai EDERY

Application No. 11/370,114

Filed: March 7, 2006

For: Method and System for Protecting a Computer and a Network From Hostile Downloadables

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 **prior patent** No. 6,092,194, 6,154,844, and 6,804,780 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☒ The undersigned is an attorney of record. Reg. No. 48,499

/Eric L. Sophir - Reg. #48,499/

May 26, 2009

Signature

Date

Eric L. Sophir

Typed or printed name

202 737 0500

Telephone Number

- ☒ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).

Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

This collection of information is required by 37 CFR 1.321. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Electronic Patent Application Fee Transmittal				
Application Number:		11370114		
Filing Date:		07-Mar-2006		
Title of Invention:		Method and system for protecting a computer and a network from hostile downloadables		
First Named Inventor/Applicant Name:		Yigal Mordechai Edery		
Filer:		Eric L. Sophir/Terry Goad		
Attorney Docket Number:		FIN0001CON1CIP1CON2		
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:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Statutory disclaimer	1814	1	140	140
Total in USD (\$)				140

Electronic Acknowledgement Receipt	
EFS ID:	5392177
Application Number:	11370114
International Application Number:	
Confirmation Number:	1442
Title of Invention:	Method and system for protecting a computer and a network from hostile downloadables
First Named Inventor/Applicant Name:	Yigal Mordechai Edery
Customer Number:	74877
Filer:	Eric L. Sophir/Terry Goad
Filer Authorized By:	Eric L. Sophir
Attorney Docket Number:	FIN0001CON1CIP1CON2
Receipt Date:	26-MAY-2009
Filing Date:	07-MAR-2006
Time Stamp:	12:55:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$140
RAM confirmation Number	8804
Deposit Account	504402
Authorized User	BEY,DAWNMARIE
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)</p>	

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	FIN0001-CON1-CIP1-CON2_Response_1181021_1.pdf	82633 7b7d024be8b9bbbed02c2adf09ab17c5f1cdfeffe	no	15
Warnings:					
Information:					
2	Drawings-only black and white line drawings	FIN0001-CON1-CIP1-CON2_ReplacementDrawing_1181062_1.pdf	313085 659d6908ebc77ca8433f33f665e7cdd176e96694	no	1
Warnings:					
Information:					
3	Terminal Disclaimer Filed	FIN0001-CON1-CIP1-CON2_TerminalDisclaimer_1181050_1.pdf	95965 a79331a3ebd1c508871ca4411900dd80ce7026	no	1
Warnings:					
Information:					
4	Fee Worksheet (PTO-875)	fee-info.pdf	29975 b4fc09ecb55aca6d85a1ebbf6d4e9571330136e7f	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			521658		
<p>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.</p> <p><u>New Applications Under 35 U.S.C. 111</u> 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.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> 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.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> 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.</p>					


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.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 11/370,114		Filing Date 03/07/2006		<input type="checkbox"/> To be Mailed		
APPLICATION AS FILED – PART I											
(Column 1)			(Column 2)		SMALL ENTITY <input type="checkbox"/>		OR		OTHER THAN SMALL ENTITY		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)		RATE (\$)	FEE (\$)				
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A					
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			N/A					
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A					
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$	=		OR	X \$	=			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$	=			X \$	=			
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).										
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))											
* If the difference in column 1 is less than zero, enter "0" in column 2.											
TOTAL											
APPLICATION AS AMENDED – PART II											
(Column 1)			(Column 2)		(Column 3)		SMALL ENTITY		OR OTHER THAN SMALL ENTITY		
AMENDMENT	05/26/2009	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)		RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	* 30	Minus	** 75	= 0	X \$	=		OR	X \$52=	0
	Independent (37 CFR 1.16(h))	* 6	Minus	***20	= 0	X \$	=		OR	X \$220=	0
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))										
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	0	
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)		RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$	=		OR	X \$	=
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$	=		OR	X \$	=
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))										
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE		
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.											
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".											
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".											
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.											

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

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

Legal Instrument Examiner:
/RAMONA D. WILSON/

Application Number 	Application/Control No. 11/370,114	Applicant(s)/Patent under Reexamination EDERY ET AL.	
Document Code - DISQ		Internal Document – DO NOT MAIL	

TERMINAL DISCLAIMER	<input checked="" type="checkbox"/> APPROVED	<input type="checkbox"/> DISAPPROVED
Date Filed : 05/26/09	This patent is subject to a Terminal Disclaimer	

Approved/Disapproved by:
Angie

U.S. Patent and Trademark Office

Form PTO-1449 (Rev. 2-32)		U.S. Department of Commerce Patent & Trademark Office		Atty. Docket No. FIN0001-CON1-CIP1- CON2		Serial No. 11/370,114	
INFORMATION DISCLOSURE STATEMENT							
(Use several sheets if necessary)				Applicant Yigal Mordechai EDERY, et al.			
				Filing Date March 7, 2006		Group 2431	
U.S. PATENT DOCUMENTS							
Examiner Initial		Document Number	Date	Name	Class	Sub- Class	Filing Date (if appropriate)
		7,418,731	8/26/08	Touboul	726	22	5/3/04
		7,343,604	3/11/08	Grabarnik, et al.	719	313	7/25/03
		7,210,041	4/24/07	Gryaznov, et al.	713	188	4/30/01
		2005/0172338	8/4/05	Sandu, et al.	726	22	1/30/04
		2006/0031207	2/9/06	Bjarnestam, et al.	707	3	6/8/05
		6,917,953	7/12/05	Simon, et al.	707	204	12/17/01
		6,598,033	7/22/03	Ross, et al.	706	46	7/14/97
		6,519,679	2/11/03	Deviredy, et al.	711	114	6/11/99
		6,487,666	11/26/02	Shanklin, et al.	726	23	1/15/99
		6,434,669	8/13/02	Arimilli, et al.	711	128	9/7/99
		6,434,668	8/13/02	Arimilli, et al.	711	128	9/7/99
		2004/0088425	5/6/04	Rubinstein, et al.	709	230	10/31/02
		2004/0073811	4/15/04	Sanin	726	13	10/15/02
		6,425,058	7/23/02	Arimilli, et al.	711	134	9/7/99
		6,339,829	1/15/02	Beadle, et al.	726	15	7/30/98
		6,088,803	7/11/00	Tso, et al.	726	22	12/30/97
		6,088,801	7/11/00	Grecsek	726	1	1/10/97
EXAMINER				DATE CONSIDERED			
EXAMINER: Initial if citation 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.							
U.S. PATENT DOCUMENTS CONT'D.							

Serial No. 11/370,114 (Docket No. FIN0001-CON1-CIP1-CON2)
Information Disclosure Statement

Page 2 of 7

		5,987,611	11/16/99	Freund	726	4	5/6/97
		5,978,484	11/2/99	Apperson, et al.	705	54	4/25/96
		5,963,742	10/5/99	Williams	717	143	9/8/97
		5,956,481	9/21/99	Walsh, et al.	726	23	2/6/97
		5,951,698	9/14/99	Chen, et al.	714	38	10/2/96
		5,892,904	4/6/99	Atkinson, et al.	726	22	12/6/96
		5,884,033	3/16/99	Duvall, et al.	709	206	5/15/96
		5,881,151	3/9/99	Yamamoto	726	24	7/20/94
		5,864,683	1/26/99	Boebert, et al.	709	249	10/12/94
		5,859,966	1/12/99	Hayman, et al.	726	23	10/10/95
		5,850,559	12/15/98	Angelo, et al.	713	320	8/7/96
		5,832,274	11/3/98	Cutler, et al.	717	171	10/9/96
		5,832,208	11/3/98	Chen, et al.	726	24	9/5/96
		5,805,829	9/8/98	Cohen, et al.	709	202	10/1/96
		5,796,952	8/18/98	Davis, et al.	709	224	3/21/97
		5,784,459	7/21/98	Devarakonda, et al.	713	165	8/15/96
		5,765,205	6/9/98	Breslau, et al.	711	203	12/27/95
		5,761,421	6/2/98	van Hoff, et al.	709	223	3/25/96
		5,740,441	4/14/98	Yellin, et al.	717	134	12/20/95
		5,740,248	4/14/98	Fieres, et al.	713	156	12/19/96
		5,724,425	3/3/98	Chang, et al.	705	52	6/10/94
		5,720,033	2/17/98	Deo	726	2	7/25/95
		5,692,124	11/25/97	Holden, et al.	726	2	8/30/96
EXAMINER				DATE CONSIDERED			
EXAMINER: Initial if citation 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.							
U.S. PATENT DOCUMENTS CONT'D.							

Serial No. 11/370,114 (Docket No. FIN0001-CON1-CIP1-CON2)
Information Disclosure Statement

Page 3 of 7

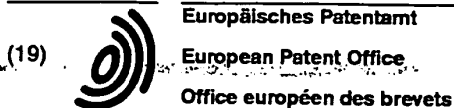
		5,692,047	11/25/97	McManis	713	167	12/8/95
		5,675,711	10/7/97	Kephart, et al.	706	12	5/13/94
		5,638,446	6/10/97	Rubin	705	51	8/28/95
		5,579,509	11/26/96	Furtney, et al.	703	27	2/8/91
		5,572,643	11/5/96	Judson	709	218	10/19/95
		5,485,575	1/16/96	Chess, et al.	714	38	11/21/94
		5,485,409	1/16/96	Gupta, et al.	726	25	4/30/92
		5,414,833	5/9/95	Hershey, et al.	726	22	10/27/93
		5,361,359	11/1/94	Tajalli, et al.	726	23	8/31/92
		5,359,659	10/25/94	Rosenthal	726	24	10/19/92
		5,077,677	12/31/91	Murphy, et al.	706	62	6/12/89
FOREIGN PATENT DOCUMENTS							
		EP 1132796	9/12/01	Universite Catholique De Louvain	G06F	1/00	3/8/00
		EP 1091276	4/11/01	Alcatel	G06F	1/00	10/6/99
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)							
		Zhong, et al., "Security in the Large: is Java's Sandbox Scalable?," <i>Seventh IEEE Symposium on Reliable Distributed Systems</i> , pp. 1-6, October, 1998					
		Rubin, et al., "Mobile Code Security," <i>IEEE Internet</i> , pp. 30-34, December, 1998					
		Schmid, et al. "Protecting Data From Malicious Software," <i>Proceeding of the 18th Annual Computer Security Applications Conference</i> , pp. 1-10, 2002					
EXAMINER				DATE CONSIDERED			
EXAMINER: Initial if citation 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.							

OTHER DOCUMENTS CONT'D. (Including Author, Title, Date, Pertinent Pages, Etc.)	
	Corradi, et al., "A Flexible Access Control Service for Java Mobile Code," <i>IEEE</i> , pp. 356-365, 2000
	International Search Report for Application No. PCT/IB97/01626, 3 pp., May 14, 1998 (mailing date)
	International Search Report for Application No. PCT/IL05/00915, 4 pp., dated March 3, 2006
	Written Opinion for Application No. PCT/IL05/00915, 5 pp., dated March 3, 2006 (mailing date)
	International Search Report for Application No. PCT/IB01/01138, 4 pp., September 20, 2002 (mailing date)
	International Preliminary Examination Report for Application No. PCT/IB01/01138, 2 pp., dated December 19, 2002
	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/
	Power, James, "Lexical Analysis," 4 pp., May 14, 2006, Retrieved from the Internet: http://www.cs.may.ie/~jpower/Courses/compilers/notes/lexical.pdf
	Sitaker, Kragen, "Rapid Genetic Evolution of Regular Expressions" [online], <i>The Mail Archive</i> , April 24, 2004 (retrieved on December 7, 2004), 5 pp., Retrieved from the Internet: http://www.mail-archive.com/kragen-tol@canonical.org/msg00097.html
	"Lexical Analysis: DFA Minimization & Wrap Up" [online], Fall, 2004 [retrieved on March 2, 2005], 8 pp., Retrieved from the Internet: http://www.owl.net.rice.edu/~comp412/Lectures/L06LexWrapup4.pdf
	"Minimization of DFA" [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
EXAMINER	DATE CONSIDERED
EXAMINER: Initial if citation 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.	

OTHER DOCUMENTS CONT'D. (Including Author, Title, Date, Pertinent Pages, Etc.)	
	"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
	"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/~hansen/classes/3813fall01/slides/06Minimize.pdf
	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
	Chang, Chia-Hsiang, "From Regular Expressions to DFA's Using Compressed NFA's," October, 1992, 243 pp., http://www.cs.nyu.edu/web/Research/Theses/chang_chia-hsiang.pdf
	"Products," Articles published on the Internet, "Revolutionary Security for a New Computing Paradigm" regarding SurfinGate™, 7 pp.
	"Release Notes for the Microsoft ActiveX Development Kit," August 13, 1996, activex.adsp.or.jp/inetsdk/readme.txt , pp. 1-10
	Doyle, et al., "Microsoft Press Computer Dictionary," Microsoft Press, 2d Edition, pp. 137-138, 1993
	Finjan Software Ltd., "Powerful PC Security for the New World of Java™ and Downloadables, Surfin Shield™," Article published on the Internet by Finjan Software Ltd., 2 pp. 1996
	Finjan Software Ltd., "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
	Finjan Software Ltd., "Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0," Las Vegas Convention Center/Pavillion 5 P5551, 3 pp., November 18, 1996
EXAMINER	DATE CONSIDERED
EXAMINER: Initial if citation 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.	

OTHER DOCUMENTS CONT'D. (Including Author, Title, Date, Pertinent Pages, Etc.)	
	Finjan Software Ltd., "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
	Finjan Software Ltd., "Java Security: Issues & Solutions," Article published on the Internet by Finjan Software Ltd., 8 pp. 1996
	Finjan Software Ltd., Company Profile, "Finjan - Safe Surfing, The Java Security Solutions Provider," Article published on the Internet by Finjan Software Ltd., 3 pp., October 31, 1996
	"IBM AntiVirus User's Guide, Version 2.4," International Business Machines Corporation, pp. 6-7, November 15, 1995
	Khare, R., "Microsoft Authenticode Analyzed" [online], July 22, 1996 [retrieved on June 25, 2003], 2 pp., Retrieved from the Internet: http://www.xent.com/FoRK-archive/smmr96/0338.html
	LaDue, M., "Online Business Consultant: Java Security: Whose Business is It?, Article published on the Internet, Home Page Press, Inc., 4 pp., 1996
	Leach, Norvin, et al., "IE 3.0 Applets Will Earn Certification," <i>PC Week</i> , Vol. 13, No. 29, 2 pp., July 22, 1996
	Moritz, R., "Why We Shouldn't Fear Java," <i>Java Report</i> , pp. 51-56, February, 1997
	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/inetsdk/help/overview.htm
	Microsoft® Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet," Microsoft Corporation, October, 1996, including Abstract, Contents, Introduction, and pp. 1-10
	Microsoft Corporation, Web Page Article "Frequently Asked Questions About Authenticode," last updated February 17, 1997, printed December 23, 1998, URL: http://www.microsoft.com/workshop/security/authcode/signfaq.asp#9 , pp. 1-13
EXAMINER	DATE CONSIDERED
EXAMINER: Initial if citation 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.	

OTHER DOCUMENTS CONT'D. (Including Author, Title, Date, Pertinent Pages, Etc.)		
		Okamoto, E., et al., "ID-Based Authentication System for Computer Virus Detection," <i>IEEE/IEE Electronic Library online, Electronics Letters</i> , Vol. 26, Issue 15, ISSN 0013-5194, July 19, 1990, Abstract and pp. 1169-1170, URL: http://iel.ihs.com:80/cgi-bin/iel.cgi?se...2ehts%26ViewTemplate%3ddocview%5fb%2ehts
		Omura, J. K., "Novel Applications of Cryptography in Digital Communications," <i>IEEE Communications Magazine</i> , pp. 21-29, May, 1990
		Schmitt, D.A., ".EXE files, OS-2 style," <i>PC Tech Journal</i> , Vol. 6, No. 11, p. 76(13), November, 1988
		Zhang, X. N., "Secure Code Distribution," <i>IEEE/IEE Electronic Library online, Computer</i> , Vol. 30, Issue 6, pp. 76-79, June, 1997
		D. Grune, et al., "Parsing Techniques: A Practical Guide," John Wiley & Sons, Inc., New York, New York, USA, pp. 1-326, 2000
EXAMINER		DATE CONSIDERED
EXAMINER: Initial if citation 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.		



(11) **EP 1 132 796 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
 12.09.2001 Bulletin 2001/37

(51) Int Cl.7: **G06F 1/00**

(21) Application number: **00104966.7**

(22) Date of filing: **08.03.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
 Designated Extension States:
AL LT LV MK RO SI

(72) Inventor: **Mas Ribès, Joan-Maria**
43206 Reus (ES)

(74) Representative:
Kirschner, Klaus Dieter, Dipl.-Phys.
Schneiders & Behrendt
Rechtsanwälte - Patentanwälte
Sollner Strasse 38
81479 München (DE)

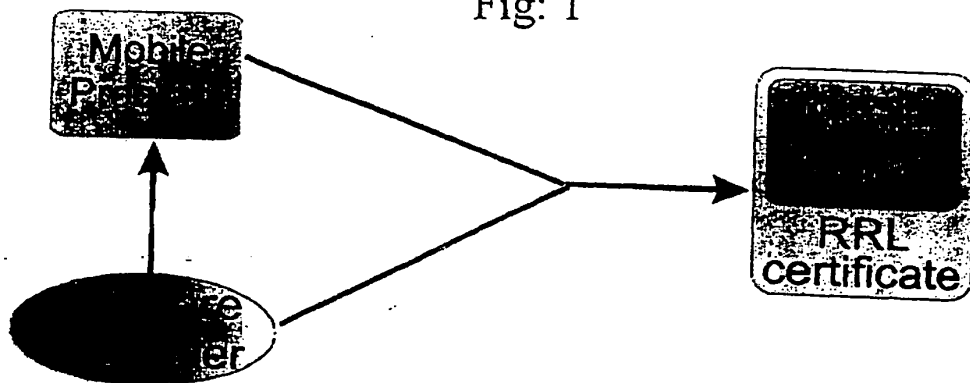
(71) Applicant: **UNIVERSITE CATHOLIQUE DE**
LOUVAIN
1348 Louvain la Neuve (BE)

(54) **Mobile code and method for resource management for mobile code**

(57) A mobile code linked to a certificate including at least a resource requirements list (RRL) including those resources needed by the mobile code to be properly executable plus those resources that are known a priori to be accessed when executing the mobile code. The unique certificate contains additionally an issuer of the certificate information identifying the entity issuing the certificate, a subject information identifying the mo-

bile code to which the certificate is referred, and a validity period information stating the period of time within which the certificate is valid. When downloading or uploading a mobile code the RRL is transferred to the user informing the user of the resource requirements of the mobile code. An execution environment is provided in an execution peer of the user, the execution environment defining at least the resource access policy that will be applied to the mobile code on execution.

Fig: 1



EP 1 132 796 A1

Description

[0001] This invention relates to a mobile code and method for resource management for mobile code.

[0002] Nowadays, with the recent explosive growth of the Internet, the number of computer interconnected in a global communications network grows exponentially. Many view the Internet as a universal communications medium that can replace telephone, television and radio. The potential is there, but progress has been hampered by the open design of the network itself. It is still too easy to intercept, monitor and forge messages on the Internet, and people are reluctant to use the network for financially or legally sensitive data.

[0003] Computer networks are evolving at a very fast pace, and this evolution proceeds along several aspects. Network links are constantly improved, and technological developments lead to increased computational power in network nodes. With increase in size and performance of computer networks, network connectivity has become a basic feature of computers and many products in the consumer electronics industry. On the other hand, users can exploit network connectivity independently of their physical location. In this new scenario, mobile users can move together with their hosts across different locations and still find their working environment.

[0004] The problems faced by users of the Internet fall into two main categories: privacy and authentication. Privacy involves transmitting messages that cannot be altered or read en route, while authentication allows each party to a communication to be sure of the identity of the other. Cryptography holds the promise of a solution to these problems.

[0005] These developments lead to a widespread diffusion of services and applications, making it necessary to increase the customizability of services. Thereby, different classes of users are then enabled to tailor the functionality and interface to a service according to their specific configuration, needs and preferences. Finally, the dynamic nature of both the underlying network infrastructure and market requirements demand higher levels of extensibility and flexibility.

[0006] There exist already a number of patent publications related to security aspects and authorizations for mobile programs. The systems described in these patent publications have, however some serious drawbacks. First, whenever certification is used, the systems require the existence of a hierarchic certification infrastructure in place. Second, all the systems deal with authorization. And finally, these patent publications all talk about low-level resource access such as file permissions, program execution, and network access. Some examples of these patent publications are discussed below.

[0007] The US 5,412,717 A relates to a computer system security method and apparatus having program authorization information data structures. The authoriza-

tion information is about low level resource access at operating system level. The only external resources available are the possibility to call another executable. Furthermore, the system needs to be implemented at an operating system level. The invention states that if all authorizations defined in the "Program Authorization Information" are not granted, the program can not be executed.

[0008] The US 5,892,904 A relates to a code certification for network transmission. A system is described to support the distribution of software over networks or off-line along with an Access Control List (ACL) for the program itself and a certificate that 'makes' the program secure for execution. In this case, the code production system submits the program and the ACL for the program to a certification authority, which sends back a certificate on the code and another one on the ACL for the program. At distribution time, the code is sent along with the ACL, the certificate on the code (which in fact is more a signature than a certificate) and another certificate on the ACL (again, this is more a signature by a CA over the ACL than a certificate). The contents of the ACL define the rights and authorizations a program has. In case not all of these authorizations are granted by the executing system or user, the program cannot run.

[0009] The US 5,892,904 A shows a system for certifying executable objects. The patent deals exclusively with program certification for network transmission. This certification guarantees program integrity, gives descriptive information on the program itself and information on the entity that certifies the program. This patent does not deal with any kind of authorization nor resource access.

[0010] The US 5,919,247 A relates to a method for the distribution of code and data updates over any network. Applications are seen as channels that can be subscribed to and updated. Whenever a user subscribes to a channel, the associated application is downloaded to the local disk and can be executed any number of times. On the other hand, there is the possibility to define an updating rate in which applications will be updated if necessary. This method basically deals with software downloading and updating and lacks, however, some important aspects on software downloading such as security and payment/licensing.

[0011] The US 5,978,484 A describes a system in which code to be sent through the network is associated with a "privilege request code", i.e. a set of rights the code may exercise, and digitally signed by a certification authority. A run-time system prevents the code from exercising unauthorized accesses. A certification hierarchy needs to be in place so that the user or executing system can verify the certificate attached to the program. The first drawback of the system is that it assumes the existence of a certification hierarchy in such a way that any user on the network can verify the validity of a given certificate. Such an infrastructure is not in place nowadays and will most likely never exist. On the other

hand, it makes the distributing authority dependent on a certification authority, which is a strong requirement.

[0012] There are also a number of scientific publications dealing mobile code handling. Examples are: D. Balfanz and L. Gong. "Experience with Secure Multi-Processing in Java". Technical Report, Princeton University, September 1997; and G. Back and W. Hsieh. "Drawing the Red Line in Java". In Proceedings of the 7th Workshop on Hot Topics in Operating Systems, March 1999. IEEE Computer Society; and G. Back, P. Trullmann, L. Stoller, W.C. Hsieh and J. Lepreau. "Java Operating Systems: Design and Implementation". Technical Report UUCS-98-015, University of Utah, August 1999; and G. Czajkowski and T. von Eicken. "JRes: A Resource Accounting Interface for Java". In Proceedings of the 1998 ACL OOPSLA Conference, Vancouver, BC, October 1998; and L. Gong, M. Mueller, H. Prafullachandra and R. Schemers. "Going Beyond the Sandbox: An Overview of the New Security Architecture in the Java Development Kit 1.2". In Proceedings of the USENIX Symposium on Internet Technologies and Systems, Monterey, CA, December 1997; and T. Tock, D. Sturman and R. Campbell. "Security, Delegation, and Extensibility". Technical Report, University of Illinois, November 1994; and T. von Eiken, C. Chang, G. Czajkowski, C. Hawblitzel, D. Hu and D. Spoonhower. "J-Kernel: a Capability-Based Operating System for Java". To appear in Secure Internet Programming: Security Issues for Distributed and Mobile Objects, Springer-Verlag Lecture Notes in Computer Science, 1999; and D. S. Wallach, D. Balfanz, D. Dean and E.W. Felten. "Extensible Security Architectures for Java". In Proceedings of the 16th Symposium on Operating Systems Principles, October 1997, Saint-Malo, France.

[0013] A few years ago, Java, developed by Sun Microsystems, triggered most of the attention and expectations on code mobility. Being able to run on any platform, Java has become a preferred research and development language for code mobility. Since then, most code mobility research literature refers to Java even if the paradigms, methodologies or concepts exposed are general and independent of any language. The Java 1.2 approach to the security of mobile code is focused exclusively on control access to resources on the machine onto which the application is executed. Classes are grouped in domains defined on the basis of the origin of the code. The address of the server providing the code or the public key associated with the signature over the code define such domains. A user can then associate to each domain an access control list containing the resources made available to classes within a domain. The Java runtime maintains a mapping from objects to their protection domains and then to their permissions. Each resource manages the permissions by itself. Nevertheless, it has some important drawbacks. Precisely, privileges are assigned to code based on their origin and totally independent of the application it implements. There is no support for resource accounting, monitoring

or reclamation, which are required from a system point of view. Furthermore, mobile code usually requires awareness of the location it is executed, and the resources and its state available to it.

[0014] Another totally different approach to resource management comes from research carried out in the past in the field of operating systems applied to type-safe languages such as Java. Type-safe languages provide the same functionality as a MMU (memory management unit) in classical operating systems, but within a single address space. The MMU is in charge of isolating address-spaces of different processes running on the same machine, and user and kernel execution modes.

[0015] Operating systems implemented with type-safe languages have several advantages over traditional operating systems with hardware-based MMU. One of the most time expensive operations on computers is context switching between user and kernel mode. These switches occur every time a user-space application makes a system call. Any operations on the file system, network access or keyboard read causes produces a context switch. Type-safe languages prevent from accessing variables or objects in an illegal way, opposed to the possibility in other languages like C/C++, in which one can access and modify the processes' memory. This feature makes unnecessary the use of MMU and boosts the performance of the system by avoiding context switching.

[0016] However, the concept of operating system limits the possibilities of such systems. The different prototypes deal exclusively with fair allocation of resources to different processes running on a machine, and provide applications with different ways to manage these resources. They lack, nevertheless, the possibility to externally define the resources available to an application.

[0017] Code mobility is exploited on an Internet scale, conceived to operate in large-scale settings with heterogeneous hosts connected by links at different bandwidths. This conception is opposed to distributed systems providing object migration that have been designed having in mind small-scale networks with high bandwidths. Mobile code is location and environment-aware and it takes actions based on such knowledge. Nevertheless, mobile code has some non-negligible risks regarding its security. A program going from computer to computer with the same privileges for the provider and the user is a non-acceptable risk for system administrators and users. Unless some precautions are taken, mobile code could read files, delete them, access the network impersonating the user or abuse of any of the resources the user has access to.

[0018] In view of the above, it is an object of the invention to provide a secured and scalable resource management at user level when using the code.

[0019] For achieving the above object, a mobile code comprises a resource usage needs section containing at least a resource requirements list (RRL) including

those resources needed by the mobile code to be properly executable plus those resources that are known a priori to be accessed when executing the mobile code. The invention provides a secure resource management for mobile code on the receiving and executing peer. A programmer or software provider/distributor attaches a RRL containing a description of the resources required by the application in order to correctly run. This information is a list of the different resources the mobile code will eventually access. The semantics of this Resource Requirements List is "the programmer of this mobile code states that the application needs to access the resources in the RRL". The goal of the RRL is not to transfer authorization but to provide a basis for the resource management.

[0020] According to a preferred aspect of the invention, the resource usage needs section of the mobile code is a certificate which is unique for each different mobile code. Out of security reasons, it is preferred to include the RRL in a certificate linked to the mobile code. For example the "most important" certificate is the certificate which is attached, for example, via a soft link by means of a hash function on the mobile code. The RRL can be contained in this certificate.

[0021] According to a preferred aspect of the invention, the resource usage needs section of the mobile code contains, in addition to the resource requirements list, any of the following information: a) issuer of the certificate information identifying the entity issuing the certificate, b) subject information identifying the mobile code to which the certificate is referred, and c) validity period information stating the period of time within which the certificate is valid. Any of this information subjects serve to further improve the ability of the system to manage resources.

[0022] According to a further preferred aspect of the invention, the information as to the issuer of the certificate is a digest of the public key of the entity having produced the mobile code. By using a digest of the public key of the entity having produced the mobile code, the safety of this information is further improved as it is made more difficult to forge the identity of this entity.

[0023] According to a further preferred aspect of the invention, the information as to the issuer of the certificate is a public key of the entity having produced the mobile code. Using the public key as an identification of the entity having produced the mobile code along with the signature on the certificate, identifies and authenticates the producer and gives a high level of security to this identification information.

[0024] According to a further preferred aspect of the invention, the subject information is a hash of the mobile code. To use a hash of the mobile code as subject information ensures again a high level of security in relation to this information. As security is an important aspect in the handling of mobile code, the importance of the last mentioned aspects of the invention is substantial.

[0025] According to a further preferred aspect of the invention, the resource requirements' list contains any of the following information: a) name of the resource information specifying the type of resource. b) action on the resource specifying as to how the resource should be used, c) upper quantitative limit information stating the maximum usage of the resource from a quantitative point of view, and d) upper qualitative limit information stating the maximum usage of the resource from a qualitative point of view.

[0026] The more information is given about the resource requirements, the better is the basis for deriving a successful and tailored management. Therefore, if anyone or several or all of this information is provided, the results management is correspondingly improved.

[0027] According to a further preferred aspect of the invention, the mobile code and the certificate are logically linked by means of the code hash. This ensures that the mobile code and the certificate containing the information necessary for performing a good resource management are not separated in any stage of their co-existence so that the mobile code can, at any time, rely on the resource management based on the logically linked certificate.

[0028] According to a further preferred aspect of the invention, certificate or a sequence of certificates is linked to the mobile code and the RRL list, the certificate or certificates transferring trust from a principal trusted by the software consumer to the RRL certificate issuer. The certificate or the sequence of the certificate contains one or several certificates transferring authorization from a executing peer to the principal who signed the certificate containing RRL. If the certificate or the certificate sequences is/are valid, the run-time execution environment will define the resource location policy. This system contributes very much to the success of the transfer and usage of the mobile code.

[0029] Furthermore, a certificate containing the RRL contains a digest of the mobile code that is used to verify its integrity which is another security feature.

[0030] According to a further preferred aspect of the invention, the mobile code comprises Java programs and applications. As mentioned before, Java provides programs and applications which are not restricted to special platforms which means that also the resource management will be platform independent.

[0031] According to a further preferred aspect of the invention, the format of the certificate or certificates is SPKI. As stated below, the SPKI is a preferred format when putting the invention to practice as SPKI provides all the features which are desirable for the invention in an efficient and elegant way.

[0032] According to a further preferred aspect of the invention, an execution program is provided in an execution environment of the user, the execution program defining at least the resource access policy that will be applied to the mobile code on execution. Such execution program will be the most suitable tool to define the re-

source access policy which also has the advantage that the implementation of the resource access policy will be done by a program which is adapted to the RRL transmitted with the mobile code.

[0033] For achieving the above object a method for resource management for mobile code using a mobile code as discussed above comprises, in the case of downloading upon request a mobile code from a principal (software provider or distributor) to a user, in a the negotiation phase in the beginning of the downloading process, a RRL list is transferred from the principle to the user informing the user of the resource requirements of the mobile code. Whenever a peer requests to download mobile code, the RRL information is used in the negotiation protocol the goal of which is to ensure that the receiving peer has all resources required for the execution of the mobile code. Exactly this information is provided by this method in a most advantageous way. Whenever a peer requests to download or upload mobile code, the RRL information can be used in a negotiation protocol. The goal of this negotiation protocol is for the sender peer to ensure that the receiving peer has all resources the mobile application requires to execute.

[0034] According to a further preferred aspect of the invention, in the negotiation phase, the downloading process further includes user and/or platform authentication, specifying restrictions imposed by the mobile code distributor as to the user and/or platform involved, and/or payment/licensing evaluation, comprising the financial aspects of the mobile code transfer. The platform authentication offers some guarantees for the software producer/distributor that is a contribution to the deal is acknowledged and the mobile code is used in the proper way.

[0035] According to a further preferred aspect of the invention, after the negotiation phase, the mobile code is downloaded. This ensures that the mobile code is downloaded and only then downloaded if all the basic requirements for its execution have already been checked and verified as being available.

[0036] According to a further preferred aspect of the invention, the mobile code or upgrades thereof are distributed from a service provider to a plurality of users, and wherein, in the case of upgrading, additional information is transmitted specifying which files need to be deleted, replaced or added. The mobile code and methods described so far can not only be used in a negotiation between two entities but also for distributing mobile code from a service provider to a plurality of users. It is advantageous that, for this application of invention, only a minimum of additional information is required which can be put into the resource usage needs section or the certificate containing the RRL.

[0037] For achieving the above object a method for resource management for mobile code using a mobile code as discussed above comprises, in the case of uploading upon request a mobile code from a resource owner to a user using a mobile code, in a the negotiation

phase in the beginning of the uploading process, a RRL list is transferred from the resource owner to the user informing the user of the resource requirements of the mobile code. Here again, the same advantages are achieved as with the downloading process.

[0038] According to a further preferred aspect of the invention, in the negotiation phase, the uploading process further includes user and/or platform authentication information specifying restrictions imposed by the resource owner as to the user and/or platform involved, and/or payment/licensing evaluation information comprising the financial aspects of the mobile code transfer. Also in the uploading process, such information is valuable to conclude an acceptable deal and to optimize the resource management.

[0039] According to a further preferred aspect of the invention, after the negotiation phase, the mobile code is uploaded. This is again to make sure that the actual transfer of the mobile code is effected only after all the security and resource management information checks have been made.

[0040] For achieving the above object, in a method for transferring mobile code through an active network for resource management for mobile code using a mobile code of as discussed above, the network comprising a plurality of active network nodes, the active flow is composed of the following information: a) a mobile code that needs to be executed in a node which is crossed by the active flow, b) a RRL-list issued by the entity that sends the mobile code to the network, c) a certificate or a sequence of certificates whose first entry is a certificate from the network operator to the starting entity, and d) the data themselves. This method ensures in a most advantageous way that the mobile code with the resource usage needs section can also be used and transferred in an environment of active networks playing an ever increasing role in the global program and data transfer.

[0041] According to a further preferred aspect of the invention, when the active flow crosses a network operator boundary from an operator X to an operator Y, the exit node of the operator X adds a certificate to the sequence issued by network operator Y authorizing operator X to send active flows through its network. This is a simple and, therefore, advantageous way to ensure a safe transfer of the mobile code with the resource usage needs section within the active networks.

[0042] According to a further preferred aspect of the invention, an execution program is provided in an execution environment of the user, the execution program defining at least the resource access policy that will be applied to the mobile code on execution. As the certificate sequence with resource usage information is attached to the mobile code, this information can be used by the receiving peer to define the resource management policy on the mobile code at run-time.

[0043] According to a further preferred aspect of the invention, the execution program is transmitted together with the mobile code. Also the execution program could

also be provided separately or on other storage media to the user, the transfer of the execution program together with the mobile code is an advantageous way of handling this matter.

[0044] According to a further preferred aspect of the invention, the method comprises any of the following steps: a) verifying that the mobile code integrity has not been compromised, b) reducing the certificate chain associated with the mobile code to verify trust transfer from the execution environment to the supplier, and c) create a process-like structure for the mobile code which isolates the mobile code from other programs running on the same execution environment.

[0045] Before executing the mobile code, the receiving peer reduces the certificate sequence that comes along with the mobile code. If the certificate or sequence of certificates is valid, the run-time execution environment will define the resource allocation policy based on the RRL along with the type of access to the resource and an upper limit on its usage. Any or all of these steps contribute to a smooth execution of the mobile code. Furthermore, the mobile programs are isolated one from each other. Also the access to resources is done through the execution environment avoiding influence or interference of mobile code and programs among each other.

[0046] According to a further preferred aspect of the invention, the resource allocation policy is defined by an intersection between the sequence of certificates, one of which contains the RRL, and the ACL local to the executing peer. In other words, authorization to access resources at run-time will be defined on the executing peer based on the RRL and the ACL of each peer and/or user. If the certificate or the certificate sequence of the certificates is valid, the run-time execution environment will define the resource location policy based on the RRL and the ACL. The ACL contains a list of principals known to the executing peer along with a maximum resource usage list per principal. Unknown principals can have a default maximum resource usage list too.

[0047] According to a further preferred aspect of the invention, the mobile code or the execution program or its reduced program is configured to discover that a given resource is available through the execution environment and to request access to it, and thus to dynamically request access to other resources, and wherein the execution environment will decide on run time whether to grant or to deny such access. One advantageous feature of the mobile code is its ability to discover the resources and other applications present or running on the target machine to be able to communicate or work with them. This gives rise to new security concerns for both the calling and the called code. Each one of them might impose its own access control based on an authenticated message exchange system, which helps to run the mobile code in a safe way. Another functionality of the execution environment is the dynamic allocation of resources not listed in the RRL. More specifically, the mo-

mobile code can dynamically discover resources on the executing peer. Therefore, the resource usage policy can be made dynamically updateable.

[0048] According to a further preferred aspect of the invention, for resources not listed in the RRL, if the resource is a build-in resource in the execution environment, the execution program will check its "run-time resource access policy" and determine, whether to grant access or not to the resource. This method takes advantage of the presence of the built-in resource and the general ability thereof.

[0049] According to a further preferred aspect of the invention, if the resource is another mobile code, this can define its own access policy stating to whom access should be granted, the advantage being that any resources which are available to anyone are integrated in the process in the execution environment almost automatically.

[0050] According to a further preferred aspect of the invention, wherein the execution program monitors and/or accounts for and/or reclaims the resources whenever its usage limit is exceeded depending on the level of trust the user has on the source of the mobile code, the resources made available to the application can be trusted to never exceed the allocated amount.

[0051] In the invention, resource needs are described and it is up to the executing environment to decide which ones are granted and which ones are not, based on their ACL and the trust path between themselves and the certifying programmer. This reflects a more generalized vision of resource as "anything a program can interact with" which is a much broader concept than the once present in the state of art. A main advantage of the invention is that it provides secure fine-grained access to resources, both quantitative and qualitative, for mobile code and that it is not restricted to provide an all or nothing access control to resources. Furthermore, in the invention, there is no need for a certificate infrastructure in order to validate the certificates or certificate sequences.

[0052] The invention also differs from the state of art specifically in that the mobile code comes along with a non-exhaustive list of required resources. The list is nevertheless only intended for execution environment information. The mobile programs could run with fewer/greater resources granted or discover new resources on the fly.

[0053] The execution environment embodying the invention allows, apart from controlling and managing access to resources, for collaboration between different programs running on this execution environment.

[0054] Embodiments of the invention are now described with reference to the attached drawings in which:

Figure 1 is a block diagram view of the software producer system depicting the phases involved in the production of a mobile pro-

- gram,
- Figure 2 shows a download upon request case in which a software consumer requests to download a mobile program from a software distributor;
- Figure 3 shows an upload upon request case in which a resource requester contacts a resource owner and asks to upload a mobile program that will act as personalized interface with the resource;
- Figure 4 shows a broadcast / multicast of mobile programs or upgrades case in which a service provider broadcasts mobile programs to offer new services to its clients or upgrades/patches;
- Figure 5 shows an active flow crossing the active network between two execution environments.
- Figure 6 shows an execution environment for mobile code.

[0055] A software producer is the entity responsible for producing a mobile code or program. This principal can be a programmer, a department within a company, an organization, etc. The mobile code is any code or application that can be sent/received through the net and is, thus, susceptible of attacking the executing peer. The mobile code can also be a local code that has arrived at the peer through a network or applications on CDROM and distributed to the users.

[0056] The first step in the process is to attach a certificate to the mobile code stating which are the resource usage needs for the given program: the software producer writes a mobile program that wants to diffuse over the Internet. To do so it needs to attach to the mobile program a certificate detailing the resource usage needs of the mobile program. This certificate is unique for each different mobile application and contains the following information:

a) Issuer of the certificate:

This is a unique identifier for the software producer. This needs not to represent a whole organization: it can be a programmer within a company, a research group or an open software group. Practically, it will be a digest (or hash) of the public key of the software producer, or the key itself.

b) Subject:

A value that uniquely identifies the mobile program to which the certificate is referred. In cryptographic words, this will be a hash of the mobile program.

c) Validity period:

This states from when to when the given certificate and thus the information contained in it is valid. This field allows for producing demo software with short validity periods, or release software with long ones.

d) Resource Requirements List (RRL):

This list should contain those resources needed by

the mobile program without which it is unable to execute, plus those resources that the software producer knows a priori that will be accessed. For each entry of the list there should be the following information which describes precisely the access to the resource:

d1) Name of the resource:

This name can be general specifying the type of resource, or more detailed, for example the resource manufacturer. The name can have constructor like 'any', or 'prefix'. For example, C:\Temp\ stands for any file in the temporary directory.

d2) Action of the resource:

A statement as to how the resource should be used. For example, if accessing a webcam, actions supported could be read (the images), zoom, on, off, focus and move.

d3) Upper quantitative limit:

This statement relates to the maximum usage of the resource from a quantitative point of view, for example writing 150Mbytes to disk or allocating 30Mbytes of memory.

d4) Upper qualitative limit:

This statement relates to the maximum usage of the resource from a qualitative point of view, for example a network connection with 10Mbits/sec, or a 4Mbits/sec video decoder.

[0057] With all the previous information, the software producer creates a certificate and attaches it to the mobile program. Here, "attach" should not be understood as a physical link, but a logical one. Precisely, a characteristic of cryptographic hashing functions is that for two different inputs, the result will be different. Moreover, it is computationally impossible, given an input, to find another one that generates the same output. Thus, mobile program and certificate are logically linked.

[0058] The certificate fields described above are those required. However, a certificate can contain some optional information such as the certification authority (entity capable of generating certificates) of the issuer, an address with detailed information on the mobile application, etc.

[0059] It should be noted that the RRL certificate is only a requirements list issued by the programmer of the mobile program. As can be seen in the following section, this certificate alone provides no security at all. Upon software distribution, the mobile program and the RRL certificate will be accompanied by a sequence of certificates transferring trust from a principal trusted by the software consumer to the RRL certificate issuer.

[0060] The distribution of mobile applications and programs can follow different patterns. In this section, different scenarios of mobile software distribution are presented. It should be noted that this section does not deal with classical software download from the Internet (ftp,

http, etc), but only with mobile applications that take advantage of the invention.

[0061] Figure 2 shows the interactions between a software distributor and a software consumer in the 'download upon request' case. A user or device contacts a software distributor and requests to download a specific piece of software. When the software distributor receives such a request, it starts a negotiation phase previous to the downloading of the mobile program. This negotiation comprehends several sub-phases:

a) User and/or platform authentication:

A software distributor may, and probably will, impose restrictions as to whom or where the software is being downloaded. Software producers or distributors may require software to be downloaded onto secure platforms that provide some guarantees as of there will not be any interference on program execution.

b) Resource requirements:

In this phase, the software distributor informs the consumer of the resource requirements on the mobile program. The objective of this phase is to avoid the downloading of software that will not be able to execute due to lack of resources. Note that the RRL is not exhaustive, since, by definition, mobile code should be able to discover resources present on the executing platform. The software consumer answers back to the distributor with a list of principals it trusts and to whom it will grant access to the resources. It is the distributor's responsibility to provide a sequence of certificates transferring trust from one of those principals to the principal that issued the RRL, along with the RRL certificate and the mobile program.

c) Payment / licensing / evaluation:

Since not all software is free of charge, this phase deals with the financial aspects of software distribution. Here, software distributor and consumer reach an agreement, possibly with proof of payment or license, before the downloading of the mobile program. Note that the consumer may be requesting an evaluation software. In this case, the only difference will be that the RRL certificate will have a short validity period, and platform authentication as described in the previous phase becomes mandatory in order to avoid illegal usage of the software.

[0062] The last step in the process is the actual download of the mobile program, the RRL certificate and a sequence of certificates that transfer trust from the software consumer down to the principal that issued the RRL certificate. Along with these data, the software distributor will most likely send a description of the mobile code with information such as name, version, etc. Software integrity is assured by the subject field in the RRL certificate which contains for example the result of a hash function on the mobile program file. If privacy is

needed, any protocol cryptographic protocol may be used.

[0063] Figure 3 shows a case in which a computer or device wants to access a resource residing on a remote computer. A resource requester contacts a resource owner and asks to upload a mobile program that will act as personalized interface with the resource. Examples of this are analyzing images of an electronic microscope or convert data from a compressed format to postscript before printing which means an application wanting to get some specific information from an electronic microscope or printing a compressed image. However, the requestor may not want to access directly the resource, but use a specific interface providing the desired functionality. This is done by sending a mobile application to the resource owner system which, in the first case, extracts locally the information from the microscope images and sends it back to the application or, in the second case, converts from a compressed image format to postscript before sending to the printer, increases the performance of the application.

[0064] The protocols between peers are basically the same as in previous case of the communication between a software distributor and a consumer, with the exception that here there is a request to upload mobile code instead of downloading. As for the negotiation phase, user and platform authentication will be used here by the resource owner, since it can have its own policy as of who can upload software to the system. On the other hand, the payment/licensing phase can be used here whenever the resource requestor should pay to access the resource. An example would be sending a mobile program that queries a remote database for which a subscription is required.

[0065] Figure 4 shows the case of a service provider with several subscribers broadcast or multicasts mobile programs to all or some of its clients. This mobile code can be whether a new mobile program that the service provider wishes to install on all its client platforms, or an upgrade/patch to already existing applications of the subscribers' systems.

[0066] Given the nature of the broadcast scenario, in this case there is not the possibility of an interactive protocol between service provider and consumers. Therefore, when the service provider broadcasts the mobile program along with some extra information:

a) Installation / upgrade information:

The installation information is basically the same information about the mobile program sent in the earlier cases. In the case of upgrading, the service provider needs to specify which files need to be deleted, replaced or added.

b) Certificate sequence:

If, in this scenario, the receiving systems are subscribed to a service and thus there is already a trust relationship, the service provider needs only to provide the sequence of certificates transferring trust

from itself to the programmer. The service provider itself may be also a software producer, in which case the certificate sequence will be empty.

c) RRL certificates and mobile program as in previous cases.

[0067] The case in which a service provider or software distributor sends a mobile program to a single receiver is a special case of the one presented above.

[0068] Active networks are a hot topic of research nowadays. The idea behind active networks is the possibility to configure each node of the network as a data flow traverses it. The active flow carries the data along with code that is executed by each active node and that does any processing on the flow. This processing can be from deciding which link the flow should follow up to reducing the quality of a video flow depending on the capacity of the link.

[0069] Figure 5 shows a scenario in which a flow between two execution environments, i.e. computers, crosses several active nodes or routers from different network operators. Any negotiation between active nodes belonging to the same or different network operators are not possible in this case. An active flow is composed of the following information:

a) The mobile code that needs to be executed in every node the flow crosses.

b) RRL certificate issued by the originating execution environment, the entity that sends the mobile code to the network.

c) A sequence of certificates whose first entry is a certificate from the network operator X to the execution environment. This certificate allows the flow to cross all active nodes belonging to operator X. When the flow crosses an operator boundary, the exit node of operator X adds a certificate to the sequence issued by network operator Y authorizing operator X to send flows through its network.

d) The data itself.

[0070] The certificates between network operators reflect real-world deals between network operators. An operator Y may authorize operator X to cross its network, but imposing some limits to the resources available to mobile code sent. In this case, there is a particular need for the active node to control the resources made available to "foreign" mobile programs.

[0071] The last phase involved in the present invention is mobile code security during execution and secured resource management. The mobile program has gotten to the executing system, or it is already present on the system. The execution environment, that is the software in charge of executing a mobile program, needs to meet some requirements so that the security of the system is not compromised (see Fig. 6). When a mobile program is launched, the execution environment performs the following steps:

a) Verify that the mobile program integrity has not been compromised. This is done by computing the hash function on the mobile program and verifying that the result is the same as in the RRL certificate.

b) Reduce the certificate chain associated with the mobile program to verify that trust is passed from the executing environment to the programmer or the issuer of the RRL certificate. To do this, the execution environment needs to access its own access control list (ACL) or the ACL of the user.

c) Define the resource access policy that will be applied to the mobile program on execution. This resource access policy is the intersection between the RRL and the ACL plus certificate sequence reduction. Note that this resource access policy refers only to those resources specified in the RRL and the ACL. Mobile programs can dynamically request access to other resources: the execution environment will decide on run-time whether to grant or deny such access.

d) Create a process-like structure for the mobile program, which isolates the program from other programs running on the same execution environment. The process abstraction also enforces the program to go through the execution environment in order to access any resource.

[0072] Whenever a mobile program requests access or tries to access a resource, the execution environment checks in the resource access policy of the process whether it has access to the resource or not. If it does, it will provide a capability that will monitor, account for and reclaim the resource whenever its usage limit is exceeded. There are, nevertheless, exception to this: low level resources, that is CPU time and memory, cannot be managed through capabilities; the execution environment manages them directly.

[0073] As stated above, the mobile code has the ability to discover the system on which it is being executed and take advantage of the resources available. This means that a program can discover that a given resource is available through the execution environment and request access to it. This resource can be a built-in resource in the execution environment or a software-based resource, i.e. any other mobile program that allows being called.

[0074] If the resource is a built-in one in the system, the execution environment will check its "run-time resource access policy" and determine whether to grant access or not to the resource. If, on the other hand, the resource is another mobile program (a video decoder or a decryption service for example) that gives access to anyone (it has not defined a its own resource access policy), access is granted too.

[0075] In case the software-based resource defines its own access policy, the execution environment will query the resource itself as to whether access is granted or not. This means that mobile programs available as

resources of a system have the ability to manage and define who (that is which mobile programs) can access them.

[0076] As stated above, security and privacy is a major concern with the handling of mobile code to cope with these requirements, one relies on cryptography. There are many different ways to implement cryptographic features in a program or on data. However, one particular format, the Simple Public Key Infrastructure or SPKI-format is particularly adapted for the purposes of the invention as will be described below.

[0077] Cryptography provides a means whereby two people can communicate openly in such a way that a third party is unable to determine or alter what is being said. By assuring privacy, cryptography indirectly provides authentication because only the communicating parties know how to encrypt and decipher each other's messages. A form of cryptography known as public-key cryptography appears to be best suited to fulfilling the requirements of the Internet. Each user of a public-key cryptosystem holds a pair of related keys. Anything encoded with one key can only be decoded by its counterpart. Each user keeps one key secret and makes the other publicly available. Thus, other people can employ the user's public key to send messages that only the user can read, or the user can "sign" a message with her private key to authenticate it - other people can apply the user's public key to verify that the message came from the user. Crucial to the operation of a global public-key cryptosystem on the Internet is a practical and reliable means of having access to the public keys, called a Public Key Infrastructure or PKI.

[0078] Much recent work has focused on moving away from identity-based PKIs to a more general system based on attributes or credentials. SPKI and SDSI (Simple Distributed Security Infrastructure) are two of such efforts. These two initiatives merged later into SPKI, given that their approach to security infrastructures and certificates were almost identical. SPKI is designed to "facilitate the construction of secure systems" and "provides simple, clear terminology for defining access-control lists and security policies". It is also an attempt to move away from identity-based certification and towards a system based on roles and credentials.

[0079] SPKI calls its entities "principals" and defines them to be digital signature verification keys. Thus, SPKI principals are public keys that can make declarations by issuing verifiable signed statements. Those signed statements come mainly in the form of certificates. SPKI provides for so called SPKI authorization certificates as a basic form of certificates which transfer some specific authorization or permission from one principal to another. Because a certificate merely transfers authorizations, rather than creating them, it is required to inject authorizations into a chain of certificates. This is done by means of ACL-entries (ACL = Access Control List). An ACL-entry lives on the machine of the verifier, leading to the observation that all authorization flow is in a

circuit - from the verifying machine's ACL, possibly through certificates and then back to the verifying machine. Alternatively, one might say that the only root of an authorization certificate chain is the verifier.

[0080] SPKI allows its principals to define groups, or sets, of principals by means of name certificates. Each group has a name and a set of members. The name is local to some principal, which is the "owner" of the group. Only a group's owner may change its definition.

A group can be an explicit list of the group's members (either as a list of principals and/or names of principals), or it can be defined in terms of other groups. Any principal can define his own groups and export them via his servers in much the same way as name bindings. The servers can issue membership certificates based on the groups' definitions.

[0081] If, from a practical point of view, mobile applications are programmed in the Java language, and programs and applications can be distributed using a specific file format that packages all files that compose the application. Moreover, this format fits the requirements of code certification, since a single file can easily be hashed to create a certificate.

[0082] As for the certificate format, SPKI certificates fit the above expressed requirements. Moreover, the fact that there is no need for an infrastructure of certification authorities in place will make the present invention easy to deploy.

Claims

1. Mobile code comprising a resource usage needs section containing at least a resource requirements list including those resources needed by the mobile code to be properly executable plus those resources that are known a priori to be accessed when executing the mobile code.
2. Mobile code according to claim 1, wherein the resource usage needs section of the mobile code is a certificate which is unique for each different mobile code.
3. Mobile code according to claim 1 or 2, wherein the resource usage needs section of the mobile code or the certificate contains, in addition to the resource requirements list, any of the following information:
 - a) issuer of the certificate information identifying the entity issuing the certificate,
 - b) subject information identifying the mobile code to which the certificate is referred, and
 - c) validity period information stating the period of time within which the certificate is valid.
4. Mobile code according to claim 3, wherein the re-

source requirements list contains any of the following information:

- a) name of the resource information specifying the type of resource, 5
 - b) action on the resource specifying as to how the resource should be used,
 - c) upper quantitative limit information stating the maximum usage of the resource from a quantitative point of view, and 10
 - d) upper qualitative limit information stating the maximum usage of the resource from a qualitative point of view.
5. Mobile code according to any of the preceding claims, wherein an execution program is provided in an execution environment of the user, the execution program defining at least the resource access policy that will be applied to the mobile code on execution. 15
6. Method for resource management for mobile code using a mobile code of any of the claims 1 to 5, wherein: 20
- (a) in the case of downloading upon request a mobile code from a principal to a user, in a the negotiation phase in the beginning of the downloading process, a RRL list is transferred from the principal to the user informing the user of the resource requirements of the mobile code, and 30
 - (b) in the case of uploading upon request a mobile code from a resource owner to a user, in a the negotiation phase in the beginning of the uploading process, a RRL list is transferred from the resource owner to the user informing the user of the resource requirements of the mobile code. 35
7. Method according to claim 6, wherein, in the negotiation phase, the downloading process further includes user and/or platform authentication, specifying restrictions imposed by the mobile code distributor as to the user and/or platform involved, and/or payment/licensing evaluation, comprising the financial aspects of the mobile code transfer; and wherein, in the negotiation phase, the uploading process further includes user and/or platform authentication information specifying restrictions imposed by the resource owner as to the user and/or platform involved, and/or payment/licensing evaluation information comprising the financial aspects of the mobile code transfer. 40
8. A method for transferring mobile code through an active network for resource management for mobile code using a mobile code of any of the claims 1 to 55

5, the network comprising a plurality of active network nodes, wherein the active flow is composed of the following information:

- a) a mobile code that needs to be executed in a node which is crossed by the active flow,
 - b) a RRL-list issued by the entity that sends the mobile code to the network,
 - c) a certificate or a sequence of certificates whose first entry is a certificate from the network operator to the starting entity, and
 - e) the data themselves.
9. Method according to claim 8, further comprising any of the following steps: 15
- a) verifying that the mobile code integrity has not been compromised,
 - b) reducing the certificate chain associated with the mobile code to verify trust transfer from the execution environment to the supplier, and
 - c) create a process-like structure for the mobile code which isolates the mobile code from other programs running on the same execution environment. 20
10. Method according to claim 8 or 9, wherein the mobile code or the execution program or its reduced program is configured to discover that a given resource is available through the execution environment and to request access to it thus to dynamically request access to other resources, and wherein the execution environment will decide on run time whether to grant or to deny such access. 25

Fig: 1

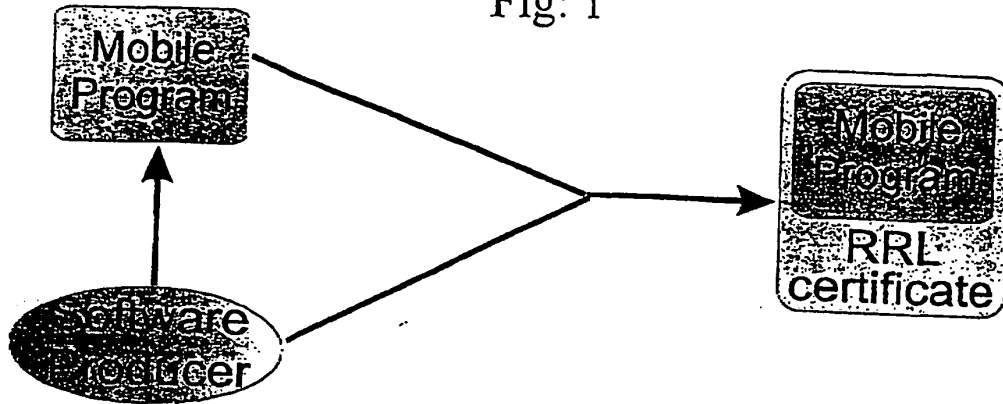
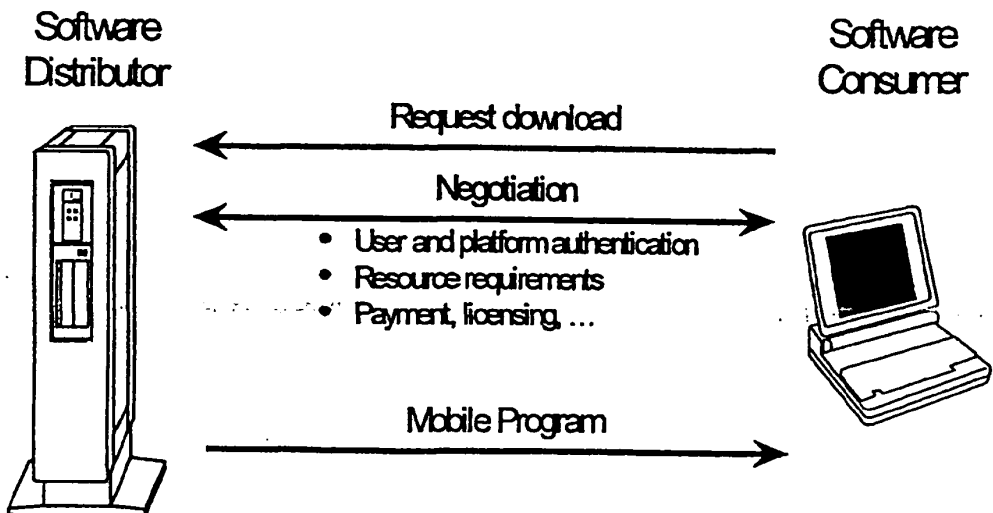


Fig: 2



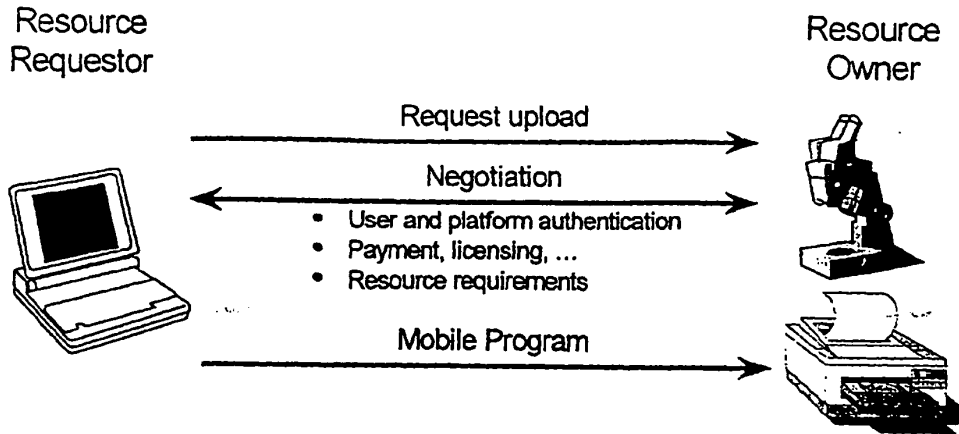


Fig: 3

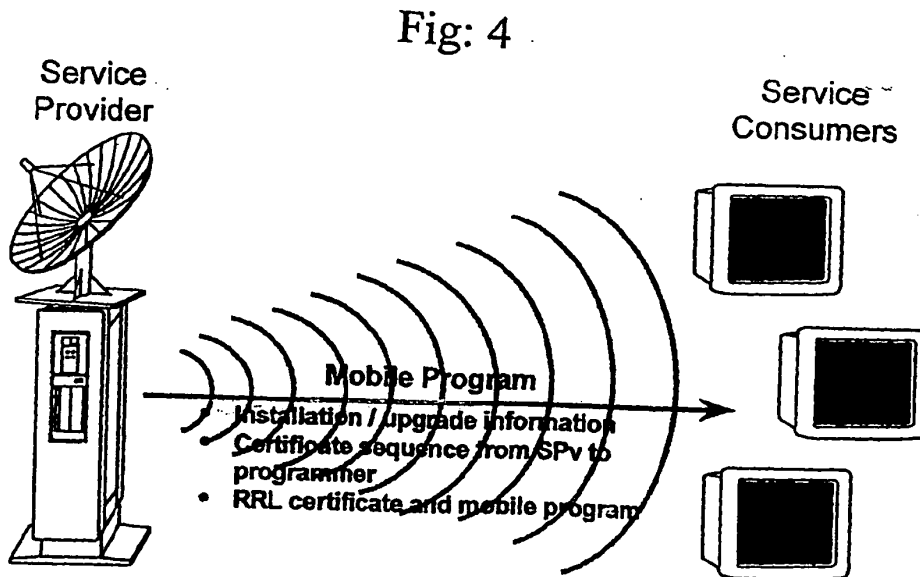


Fig: 4

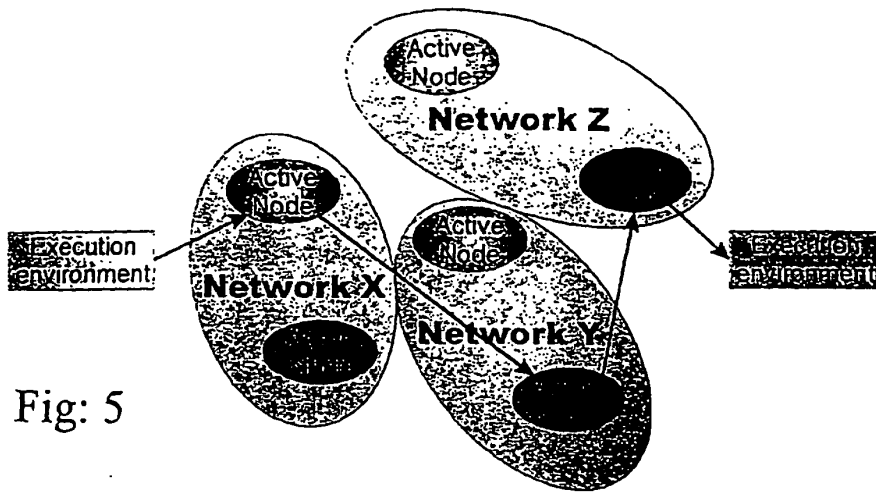
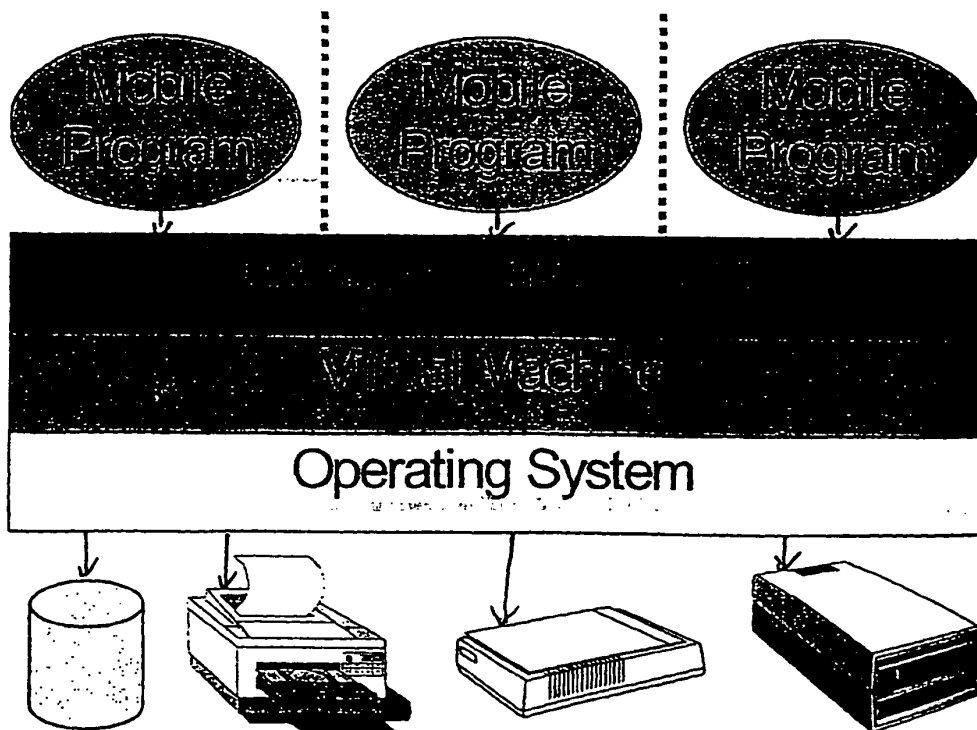


Fig: 5

Fig: 6





European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 10 4966

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (InCL1.7)
X	EP 0 813 132 A (IBM) 17 December 1997 (1997-12-17) * abstract; figures 1-3 * * page 2, line 59 - page 3, column 57 * * page 4, line 40 - page 5, line 4 *	1-4	G06F1/00
Y	—	6,7	
X	EP 0 813 133 A (IBM) 17 December 1997 (1997-12-17) * abstract * * column 3, line 5 - column 4, line 7 * * column 6, line 33 - line 50 *	1-3,5	
A	—	8,9	
Y	WO 98 07085 A (SMITH BENJAMIN HEWITT; SMITH FRED HEWITT (US); BEN SMITH INC (US)) 19 February 1998 (1998-02-19) * abstract; figures 1,3 * * page 4, line 2 - page 5, line 14 * * page 9, line 1 - page 10, line 27 *	6,7	
			TECHNICAL FIELDS SEARCHED (InCL1.7)
			G06F
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 20 December 2000	Examiner Sigolo, A
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

EPO FORM 1503 (03.02.92) (P04C01)

EP 1 132 796 A1

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 00 10 4966

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

20-12-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0813132 A	17-12-1997	US 5825877 A	20-10-1998
		JP 10083310 A	31-03-1998
EP 0813133 A	17-12-1997	JP 10091427 A	10-04-1998
WO 9807085 A	19-02-1998	US 6067582 A	23-05-2000
		AU 3793997 A	06-03-1998
		EP 0978023 A	09-02-2000

EPO FORM P0439

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
11.04.2001 Bulletin 2001/15

(51) Int. Cl.⁷: **G06F 1/00, H04L 29/06**

(21) Application number: **99440269.1**

(22) Date of filing: **06.10.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **ALCATEL**
75008 Paris (FR)

(72) Inventor: **Brette, Marc**
67408 Illkirch Cedex (FR)

(74) Representative:
Menziotti, Domenico, Dipl.-Ing et al
Alcatel
Intellectual Property Department, Stuttgart
70430 Stuttgart (DE)

(54) **Authentication of hypertext kind of resources through signature handling protocol**

(57) Method of receiving a resource out of an application stored by a service provider on a site at a client terminal, both being interconnected. The method is advantageously implemented into the browser of the client. It comprises the steps of:

- requesting the resource within the application on the site from the client terminal;
- receiving a signed archive file containing the requested resource by the client terminal;
- authenticating the received signed archive file;
- retrieving the requested resource out of the received archive file if that was undoubtedly authenticated.

EP 1 091 276 A1

Description

[0001] This invention relates to a method of receiving a resource as set forth in the preamble of claim 1, to a computer readable medium having a program recorded thereon and to a trustable disposal of a resource as set forth in the preamble of claim 10.

[0002] In the last ten years, networks of computerized terminals are more and more interconnected over the world. The set of those networks are called internet. They allow a transfer of data from one terminal to another almost everywhere as long as the terminals are connected to the same internet. The popularity of such "communication" was boosted by the introduction in the middle of the ninetieth of the so called World Wide Web (the "Web"). It is a decentralized, electronic database service offering an ensemble (universe) of dynamically connected information on the internet which win through and is called the Internet. Such information can be in any of various media and is relatively easily found by and made accessible to individuals exploring ("surfing") that universe ("Web space"). More specifically, the Web is a distributed, hypertext system comprising hypermedia documents, Web servers and Web clients.

[0003] Web clients include software programs commonly known as browsers. Browsers typically reside on an individual's electronic terminal (e.g. personal computer, laptop and in the near future even phone terminal) and, among other things, provide for exploring the Web so as to find and access Web documents.

[0004] Web servers are server processes running at a Web site i.e. a terminal connected to the Internet. The Web servers support various features, including being compatible with one or more standard protocols, e.g., the HyperText Transfer Protocol ("HTTP"), the well-known, native protocol of the Web generally unifying its information. With that programs hypermedia documents are put on the Web and resources associated with applications stored by the server on the site are let available to clients. The Web servers do not only make documents and resources accessible to clients, but also direct specific documents to clients and complete transactions responsive to each client's request which were activated through their browsers.

[0005] Web documents ("pages") are constructed in conformity with one of various accepted formats or languages, e.g., HyperText Markup Language ("HTML"). The formats support, among other things, the Web's hypermedia and hypertext characteristic. As to the hypermedia characteristic, Web documents can, and generally do, combine content from one or more of the various media including text, graphics, audio and video. As to the hypertext characteristic, Web documents can, and generally do, contain electronic links to related Web documents. Selecting the link causes the browser to (i) connect to a server associated with that link, (ii) request the linked document and (iii) if the client satisfies the server's security requirements, receive and

display the document.

[0006] The security of information and transaction transferred under that way has been identified as a significant problem. At the center of the problem are so-called crackers: individuals who seek to access computers, such as sites (servers), so as to conduct pranks, vandalism, espionage or other illegitimate activities. A way to respond to these activities, among other things is to strive to maintain the confidentiality and integrity of information, both as resident on servers and as communicated in Web transaction. Increasing the vulnerability to crackers is that the Web is an open system available to anyone in possession of readily available, affordable technology.

[0007] One important Web security issue is authentication. An example of an authentication on the Web is given by the SSL (Secure Sockets Layer) Handshake Protocol which was developed by Netscape Communications Corporation. The protocol supports server and client authentication. The SSL protocol is application independent, allowing protocols like HTTP, FTP (File Transfer Protocol), and Telnet to be layered on top of it transparently. The SSL protocol is able to negotiate encryption keys as well as authenticate the server before data is exchanged by the higher-level application. But the SSL protocol maintains the security and integrity only of the transmission channel. It uses encryption, authentication and message authentication codes only to authenticate the sites of the Web server as well as the Web client. The trust is then granted on a site by site basis.

[0008] That protocol does not authenticate the whole data itself which will be exchanged through the Internet and thus does not work against software virus like "Trojan horses". The later denominates some code put somewhere but mainly at the end of a data by an illegitimate one. Once the data is downloaded, the Trojan horse can be activated by the client unintentionally. Some special and very feared cases of Trojan horses are the so called "mockingbirds". They permit to intercept communication (especially login transactions) between the client and the server. When activated, the code will provide system-like responses to the client while saving their responses (especially account IDs, passwords and PINs).

[0009] An object of the invention is to ensure that any transaction between a trusted site and a client both interconnected is free of any kind of software virus, and to provide methods to implement such measures without losing the comfort of a service like the Web.

[0010] These objects are attained by a method of receiving a resource as claimed in claim 1, a computer readable medium as claimed in claim 9 and a trustable disposal of resources as claimed in claim 10.

[0011] It is extremely hard to ensure that platforms like Web servers are visited only by trusted clients. A site manager, the one responsible for the maintenance of a site, can never be completely sure that none imper-

sonator will achieve to penetrate a protected Web server. It is also difficult to protect a single application (Web page) with all the resources embedded in it. This explains the interest to protect the whole content of the resources which may be downloaded during a critical transaction e.g. like a banking transaction or an electronic commerce application.

[0012] The basic idea of the invention consists of assembling resources which shall be downloaded together with their respective application into a single file, "an archive file". To sign these files in their entire content ensures then that nowhere in the data's of one resource is hidden some virus. These signed files are stored on a site and let to the disposal of some potential clients able to authenticate the signature.

[0013] When a client surfing on the Web will come across one of such a resource, he may be interested to open it. This will necessarily means that before being activated on its terminal, it must be downloaded. Using its browser on its terminal on which advantageously a protocol according to the invention is running, he will request the chosen resource. This will start the protocol which will look after the corresponding archive file of that resource onto the site where the resource was found. After a download of the entire signed archive file onto the client terminal, the protocol will have to authenticate the signature of that file. Only in the positive case that it was entirely authenticated, the protocol will retrieve the requested resource out of the archive file, to active it on client terminal.

[0014] With that protocol, the client can trust not only the site itself, like it would be the case if its browser would use only a SSL protocol, but will be sure that the activation of that resource on its own terminal will not activate a virus hidden somewhere into the data's of that resource. The solution obtained with that invention permits to combine the flexibility of a service like the Web with a communication between client terminal and sites free of any transfer of virus specially of the feared mock- ingbirds.

[0015] Further advantageous features of the invention are defined in the dependent claims and will become apparent from the following description and the drawing.

[0016] One embodiment of the invention will now be explained in more detail with reference to the accompanying drawing, in which:

Fig.1 is a flow chart showing steps associated with the method of receiving a resource of a resource according to the invention.

[0017] The present invention concerns a trustable activation of some resources downloaded out of some site and methods therefore. A service provider who wants to let on a site resources all trustfully free of any virus to the disposal of some clients, will have to apply the following procedure. The codes of these resources

must be assembled in an archive file. Some times, it is of advantage to include also the codes of the corresponding application into the archive file. To build that archive file, already existing archive formats like tar, zip or jar can be used. The later is applied specifically for an ensemble of files written in an objected oriented syntax like "java", the one used for most of the resources of applications on the Web.

[0018] In some header of the archive file may be stored the information of their content. Afterwards, the archive file must be protected from the illegitimate implementation of subsidiary codes like the one of a mockingbird. This is achieved by signing the entire content of the archive file.

[0019] There exists several possibilities to perform a signature of a file. One way which would be quite advantageous in the context of this invention is the use of an encryption scheme. A particular popular one due to the ease of its utilization, is the so called public-key encryption.

[0020] This encryption scheme is based on a pair of "keys". One of them is called a public key and the other one a private key. The public key is published, while the private key is kept secret. The need for the signer (e.g. some service provider like e.g. the some credit card company) and the receiver (e.g. the browser of some client) to share secret information is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. In this system, it is no longer necessary to trust the security of some means of communications. The only requirement is that public keys be associated with their users in a trusted (authenticated) manner (for instance, in a trusted directory).

[0021] For the purpose of the invention, the archive files are encrypted using the private key of the service provider. If for example, a company wants to let to the disposal of its clients some information trustfully free of viruses on the Internet, they must be signed using the private key of that company. For that, the archive file containing the code containing this information (e.g. a resource of some application) will be encrypted. The signer don't need to care who will read this information or even visit the site where it is let to the disposal since its signature can't be imitated. This will ensure the one (e.g. some client) who will decrypt that signed archive file using a public key, of the absence of any fake code. No third-party could have modified the signed archive file without destroying the whole file.

[0022] To optimize the downloading i.e. avoiding any delay or unnecessary checking procedure, it is of great advantage for the client to install a protocol according to the method of the invention onto its browser e.g. in an URL syntax (Universal Resource Locator) as below:

(URL: signed.protocol: //host/path?resource).

Where protocol is the underlying protocol used to

retrieve the archive file. It may be for example http, https, ftp or file. Host is the name of the server where the jar file is located (it may be empty for local file). Path is the location of the jar file on the host for the given protocol. Resource is the actual name of the resource inside the jar file.

Example:

signed.http://www.alcatel.com/applets/smart-card.jar?index.html

[0023] On Fig. 1, is shown a flow chart that depicts an example of the downloading method according to the present invention. As already said above, it can be implemented on the browser of client's terminal. The method starts 10 by an action of the client onto its terminal like choosing an Internet address out of an address book e.g. stored by its browser.

[0024] In step 11, the client requests access of a Web server site by sending the Web location (Internet address) he choose when starting. Such location may be in the form of a URL. In this step, a secure communication channel may be established between the client terminal and the site. For example, if SSL is employed, the secure communication channel is established during the SSL handshake, including by, among other things, (i) negotiating an encryption algorithm between the site and the terminal and (ii) authenticating the site to the client terminal. But the building of a secure communication channel is no more of priority since the resources are anyway protected according to the invention.

[0025] In step 12, the client requests a specific resource within an application to be activated on its terminal. This will bring the browser of the client to look after the corresponding archive file 13. After finding it, the transfer 14 of that file will occur through the communication channel.

[0026] When the archive file is downloaded onto the client terminal, the authentication procedure 15 of its signature will start. The browser will apply some decryption scheme in accordance to the one used to encrypt it.

[0027] Dependent on the result of that procedure 15, will depend if the resource is taken out of the archive file or not. In the negative case, that the signature was not entirely recognized, it will mean that either the client is not allowed to download the requested resource or some codes in the archive file were illegitimately modified or added, then the archive file will be deleted 16 from the client terminal. Optionally, the protocol will contain the step 17 to send a message to the client to warn him about the result of the authentication and/or to send to the site a message 18 informing the signer of that resource and/or site manager that someone tried unsuccessfully to download some resources.

[0028] Alternatively, if the downloaded archive file was decrypted successfully, then the browser will look 19 for the requested resource into the downloaded

archive file. It will then activate the resource onto the client terminal 20. The protocol will then end its procedure 21.

[0029] The steps described above can be configured to support various options, without departing from the principles of the invention to assemble all resources of sensible applications into a single archive file protected by a signature and ready to be downloaded.

[0030] The fact to implement the protocol onto the client browser, enable to perform the procedure in an almost transparent way. The client will not necessarily notice the take place of the authentication of the requested resource. He will even not know that the resource is somewhere archived on some signed file. It is the browser which will apply the protocol after the invention by first authenticate the signed archive file. If it succeeded, it will then retrieve the requested resource out of the archive file and activate it. All the steps may take a fraction of time mainly dependent on the transfer rate on the communication channel between the site of the Web server and the client terminal.

[0031] It is therefore particularly adapted for Web pages (applications on some site) which often contain a certain number of applets (resources made of java codes). They are some times part of the application user interface and are usually downloaded and dynamically generated. Applying the procedure according to the invention ensure that the whole application user interface does not contain any fake codes put there by some impostor. It is an ideal procedure for any application but some highly secure applications such as electronic commerce applications (electronic banking service or smart card facilities). The method according to the invention can be used also if the corresponding signed archive file is downloaded out of some untrustworthy site, since the entire content of the resource is itself protected. The author of the resource has the assurance that every reader of its resource will really read the information he put there himself.

Claims

1. Method of receiving a resource out of an application stored by a service provider on a site at a client terminal, both being interconnected, the method comprising the step of
 - requesting the resource within the application on the site from the client terminal; and
 - characterized by the additional steps:
 - receiving a signed archive file containing the requested resource by the client terminal;
 - authenticating the received signed archive file;
 - retrieving the requested resource out of the received archive file if that was undoubtedly authenticated.

2. Method of receiving a resource as claimed in claim 1, characterized in that the entire requested resource is signed.
3. Method of receiving a resource as claimed in claim 1, characterized in that the signature of the archive file is authenticated using a decryption scheme. 5
4. Method of receiving a resource as claimed in claim 1, characterized in that the service provider is part of a decentralized, electronic database service offering an ensemble of dynamically connected information like the Web. 10
5. Method of receiving a resource as claimed in claim 1, characterized in that it works transparently for the client. 15
6. Method of receiving a resource as claimed in claim 1, characterized in that the requested resources are object oriented resources like java applets. 20
7. A computer readable medium having a program recorded thereon, said computer readable medium comprising computer program code means adapted to perform all the steps of claim 1 when said program is run on the client terminal. 25
8. A computer readable medium as claimed in claim 7, characterized in that the program code is built with an Universal Resource Locator syntax. 30
9. A computer readable medium as claimed in claim 7, characterized in that the program code is implemented into a browser on the client terminal. 35
10. Trustable disposal of a resource from an application on a site to some client having a terminal interconnected with the site characterized in that the resource is stored in a signed archive file on the site. 40
11. Trustable disposal of a resource as claimed in claim 10, characterized in that the archive file is signed using an encryption scheme. 45

50

55

5

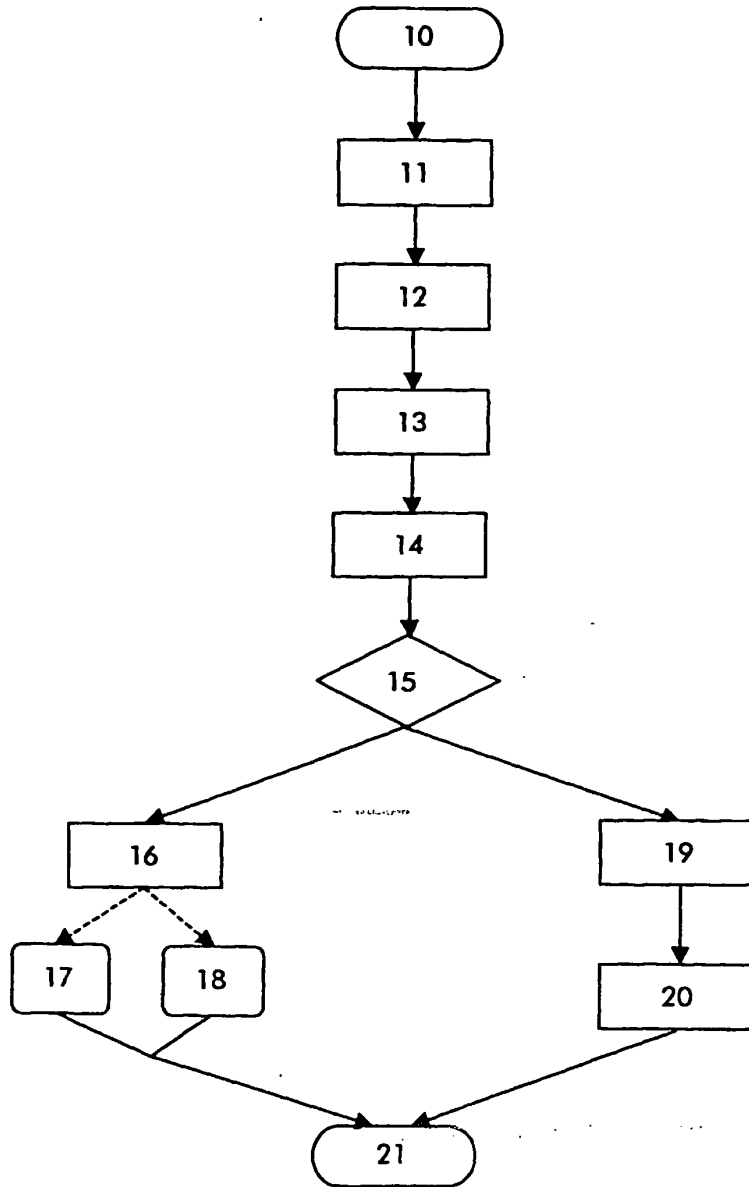


Fig.1



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 44 0269

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 892 904 A (ATKINSON ROBERT G ET AL) 6 April 1999 (1999-04-06) * abstract * * figures 2A,3,4,5,6 * * column 1, line 35 - column 3, line 36 * * column 5, line 14 - column 6, line 43 * * column 7, line 11 - column 7, line 30 * * column 11, line 9 - column 11, line 36 * * column 26, line 38-54 *	1-11	G06F1/00 H04L29/06
X	WO 98 44402 A (BRAMHILL IAN DUNCAN ;SIMS MATTHEW ROBERT CHARLES (GB); BRITISH TEL) 8 October 1998 (1998-10-08) * abstract * * figures 3,5 * * page 2, line 12 - page 4, line 29 * * page 6, line 16-22 * * page 9, line 15 - page 14, line 9 *	1,3-5	
A	EP 0 913 769 A (SUN MICROSYSTEMS, INC.) 6 May 1999 (1999-05-06) * abstract * * figures 1,2 * * page 2, line 21-29 * * page 4, line 20-27 * * page 4, column 42-43 * * page 7, line 42 - page 8, line 1 * * page 8, column 47-48 *	1,4-6	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G06F H04L
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 27 January 2000	Examiner Sigolo, A
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document</p>			

EPO FORM 1503 03.82 (P0401)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 99 44 0269

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

27-01-2000

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5892904	A	06-04-1999	NONE	
WO 9844402	A	08-10-1998	AU 6414098 A EP 0970411 A	22-10-1998 12-01-2000
EP 0913769	A	06-05-1999	US 5966702 A	12-10-1999

EPO FORM P0448

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

From the
INTERNATIONAL SEARCHING AUTHORITY

PATENT COOPERATION TREATY

REC'D 07 MAR 2006

WIPO

PCT

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

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

Applicant's or agent's file reference		Date of mailing (day/month/year)
P-9039-PC		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:

- | | | |
|-------------------------------------|--------------|--|
| <input checked="" type="checkbox"/> | Box No. I | Basis of the opinion |
| <input type="checkbox"/> | Box No. II | Priority |
| <input type="checkbox"/> | Box No. III | Non-establishment of opinion with regard to novelty, inventive step and industrial applicability |
| <input type="checkbox"/> | Box No. IV | Lack of unity of invention |
| <input checked="" type="checkbox"/> | Box No. V | Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement |
| <input type="checkbox"/> | Box No. VI | Certain documents cited |
| <input type="checkbox"/> | Box No. VII | Certain defects in the international application |
| <input type="checkbox"/> | 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 66.1bis(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 Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Date of completion of this opinion 05 February 2006 (05.02.2006)	Authorized officer <i>Ayaz Sheikh</i> Ayaz Sheikh 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:

Form PCT/ISA/237(Box No. I) (April 2005)

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 <u>NONE</u>	YES
	Claims <u>1-43</u>	NO
Inventive step (IS)	Claims <u>NONE</u>	YES
	Claims <u>1-43</u>	NO
Industrial applicability (IA)	Claims <u>1-43</u>	YES
	Claims <u>NONE</u>	NO

2. Citations and explanations:

Please See Continuation Sheet

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IL05/00915

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

Form PCT/ISA/237 (Supplemental Box) (April 2005)

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/IL05/00915

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 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).

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 grammatical 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 grammatical 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 generator 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 grammatical 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).

PATENT COOPERATION TREATY

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)

REC'D 31 DEC 2002

WIPO PCT


Applicant's or agent's file reference 134943.0 SZ	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/IB 01/ 01138	International filing date (day/month/year) 17/05/2001	Priority date (day/month/year) 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 30/11/2001	Date of completion of this report 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

Form PCT/IPEA/409 (cover sheet) P20476 (October 2002)



**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No.PCT/ IB 01/ 01138

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).

Electronic Patent Application Fee Transmittal				
Application Number:		11370114		
Filing Date:		07-Mar-2006		
Title of Invention:		Method and system for protecting a computer and a network from hostile downloadables		
First Named Inventor/Applicant Name:		Yigal Mordechai Edery		
Filer:		Dawn-Marie Bey./Jeanne Paolella-Bald		
Attorney Docket Number:		FIN0001CON1CIP1CON2		
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:				

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

Electronic Acknowledgement Receipt	
EFS ID:	5636864
Application Number:	11370114
International Application Number:	
Confirmation Number:	1442
Title of Invention:	Method and system for protecting a computer and a network from hostile downloadables
First Named Inventor/Applicant Name:	Yigal Mordechai Edery
Customer Number:	74877
Filer:	Dawn-Marie Bey./Jeanne Paolella-Bald
Filer Authorized By:	Dawn-Marie Bey.
Attorney Docket Number:	FIN0001CON1CIP1CON2
Receipt Date:	02-JUL-2009
Filing Date:	07-MAR-2006
Time Stamp:	15:27:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$180
RAM confirmation Number	1837
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	----------------------------------	------------------	------------------

1	Transmittal Letter	fin0001con1cip1con2_suppidst rans.pdf	101668 e30876c5527ecd61ae4de266a961adaa348e4dd	no	2
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Filed (SB/08)	fin0001con1cip1con2_1449frm .pdf	146028 c4e1fd91372583bc1bf2ad8bd824251d5d4fdd	no	7
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
3	Foreign Reference	fin1_ref1.pdf	2893701 62faabda68203880f1ecd0e65c2623a558a2dbb7	no	17
Warnings:					
Information:					
4	Foreign Reference	fin1_ref2.pdf	1060413 7c2aaec276b6db32773cddb2c3e8775b45ad45d5	no	8
Warnings:					
Information:					
5	NPL Documents	fin1_ref3.pdf	769016 7df75cb6443045201ef1c7ff7517e241caf7e7a6	no	6
Warnings:					
Information:					
6	NPL Documents	fin1_ref4.pdf	957228 9f9009a2cc7dc8a28422425cd0c1259efe077850d	no	5
Warnings:					
Information:					
7	NPL Documents	fin1_ref5.pdf	1959408 40d7cae891ddc83674cd0fd15248514dac6da5d8d	no	10
Warnings:					
Information:					
8	NPL Documents	fin1_ref6.pdf	1905210 99e0e0ef3d300b1934fa386678884d508730a421	no	10
Warnings:					
Information:					
9	NPL Documents	fin1_ref7.pdf	348189 1aeb15244003d0fa74f39687c2dc8391908a40df	no	3

Warnings:					
Information:					
10	NPL Documents	fin1_ref8.pdf	327971	no	4
			f00825b757bed5fca61b5cb84f874e73655904c		
Warnings:					
Information:					
11	NPL Documents	fin1_ref9.pdf	708458	no	5
			be9e3d757a0ee73f0cb32844c14eba872943400		
Warnings:					
Information:					
12	NPL Documents	fin1_ref10.pdf	402319	no	4
			06184df5efc04feb35419a604c878162efcb936		
Warnings:					
Information:					
13	NPL Documents	fin1_ref11.pdf	196337	no	2
			5932095d796e66354f062323cb902c5a78ee11da		
Warnings:					
Information:					
14	NPL Documents	fin1_ref12.pdf	631001	no	18
			114c83a1d7a6c8955d7243a9d29537409f99c27d		
Warnings:					
Information:					
15	NPL Documents	fin1_ref13.pdf	564707	no	4
			6d015ca6e4322c79668d6d78ccd522805851a95d		
Warnings:					
Information:					
16	NPL Documents	fin0001_ref14.pdf	176198	no	5
			785aa64f221f6c3a93d71f4cd56aebdafaee514e		
Warnings:					
Information:					
17	NPL Documents	fin1_ref15.pdf	836155	no	8
			d0ed6d7dcde54ced24c36c5b994e05f4d75697bb		
Warnings:					
Information:					
18	NPL Documents	fin1_ref16.pdf	151825	no	7
			e043fa5dff99a1d2d2f5a6bdeffff415a8e94ff		

Warnings:					
Information:					
19	NPL Documents	fin1_ref17.pdf	86660 0d7bfddd5bd46a6b4b6a7ff65144015bf8cbee29	no	4
Warnings:					
Information:					
20	NPL Documents	fin1_ref18.pdf	263838 1e004b4efad0bcf0bb3e168c8964045e7e1c15aab	no	3
Warnings:					
Information:					
21	Fee Worksheet (PTO-875)	fee-info.pdf	30215 4eefd1904d2e6dae7f46efd8b421c5d741b6d7da	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			14516545		
<p>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.</p> <p><u>New Applications Under 35 U.S.C. 111</u> 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.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> 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.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> 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.</p>					

Docket No. FIN0001-CON1-CIP1-CON2

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Yigal Mordechai EDERY, et al.

Serial No.: **11/370,114**

Group Art Unit: **2431**

Filed: **March 7, 2006**

Examiner: **Christopher A. Revak**

For: **METHOD AND SYSTEM FOR PROTECTING A COMPUTER AND A
NETWORK FROM HOSTILE DOWNLOADABLES**

**SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT
UNDER 37 C.F.R. §§ 1.97 AND 1.98**

U.S. Patent and Trademark Office
Customer Window, Mail Stop Amendment
Randolph Building
401 Dulany Street
Alexandria , VA 22314

Sir:

In accordance with the requirements of 37 C.F.R. §§ 1.56, 1.97-1.98 and MPEP § 609,
the references noted on the attached Form PTO-1449 are hereby brought to the attention of the
Examiner.

Since this statement is being filed after receipt of an Office Action, a fee of \$180.00 is
enclosed pursuant to 37 C.F.R. § 1.17(p). However, the Commissioner is hereby authorized to
charge any additional fees which may be required, or to credit any overpayment, to Deposit
Account No. 50-4402.

The above information is presented so that the United States Patent and Trademark
Office may, in the first instance, determine any materiality thereof to the claimed invention. See

U.S. Serial No.: 11/370,114
Information Disclosure Statement

- 2 - Docket No. FIN0001-CON1-CIP1-CON2

37 C.F.R. §§ 1.104(a) conferring the PTO duty to consider and use any such information. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

Respectfully submitted,

Date: July 2, 2009

By: /Dawn-Marie Bey - 44,442/
Dawn-Marie Bey
Registration No. 44,442

KING & SPALDING LLP
1700 Pennsylvania Avenue, N.W.
Suite 200
Washington, DC 20006
(202) 737-0500

15157/105016
Doc. No. 1214250

Electronic Acknowledgement Receipt	
EFS ID:	5637266
Application Number:	11370114
International Application Number:	
Confirmation Number:	1442
Title of Invention:	Method and system for protecting a computer and a network from hostile downloadables
First Named Inventor/Applicant Name:	Yigal Mordechai Edery
Customer Number:	74877
Filer:	Dawn-Marie Bey./Jeanne Paolella-Bald
Filer Authorized By:	Dawn-Marie Bey.
Attorney Docket Number:	FIN0001CON1CIP1CON2
Receipt Date:	02-JUL-2009
Filing Date:	07-MAR-2006
Time Stamp:	15:46:44
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	NPL Documents	fin1_ref19.pdf	2623837 ce1b1932419330a5e85cc00b0689157d76e5ee04	no	38

Warnings:

Information:

2	NPL Documents	fin1_ref20a.pdf	8357715 3aacb305df8a78bf38b66300f2c1bea171e043d4	no	112
Warnings:					
Information:					
3	NPL Documents	fin1_ref20b.pdf	7889132 03e897596b07b5e49ec52117fab2de9af6685158	no	131
Warnings:					
Information:					
4	NPL Documents	fin1_ref21.pdf	1011957 7265eff4d46451c5881738647c0b9137e8f53606	no	7
Warnings:					
Information:					
5	NPL Documents	fin1_ref22.pdf	1382230 c652cc14513627194531e853d910abf4664e32b3	no	11
Warnings:					
Information:					
6	NPL Documents	fin1_ref23.pdf	501400 46fe30954af4741fd54a9827576e6210858da075	no	4
Warnings:					
Information:					
7	NPL Documents	fin1_ref24.pdf	247810 4ea73f27fef57c20de6e740b4c0a18f61df27f32	no	2
Warnings:					
Information:					
8	NPL Documents	fin1_ref25.pdf	269981 083fd42207c172504775ab55b41cf2099c1ea27	no	2
Warnings:					
Information:					
9	NPL Documents	fin1_ref26.pdf	386316 683235a2b5434c14bf003b6aab3ebe7dd8b3278	no	3
Warnings:					
Information:					
10	NPL Documents	fin1_ref27.pdf	214821 3e5d10fc7848ec1945b08bd51c130ee1d50f8e99	no	1
Warnings:					
Information:					

11	NPL Documents	fin1_ref28.pdf	990631 a8f323f57172a0fc5c39b0071107f5b13a7c58af	no	8
Warnings:					
Information:					
12	NPL Documents	fin1_ref29.pdf	454867 002824525117c873234e7903f3638c6611468278	no	3
Warnings:					
Information:					
13	NPL Documents	fin1_ref30.pdf	333646 1300ab3d3cd0d136fa333b427ee06d9109368d37	no	3
Warnings:					
Information:					
14	NPL Documents	fin1_ref31.pdf	269134 c9a152886f70a2309cabbfe9184fd4c003dbed0c	no	2
Warnings:					
Information:					
15	NPL Documents	fin1_ref32.pdf	694449 f8c2b7976ee3ef4ba885de6e7441506d2e5eb1d4	no	4
Warnings:					
Information:					
16	NPL Documents	fin1_ref33.pdf	315045 41b803ca841cedbfb81a9ed36c863641d94aa9cc6	no	2
Warnings:					
Information:					
17	NPL Documents	fin1_ref34.pdf	1234532 aa9f112842edba30a396c1c2b729f5a995e632b4	no	6
Warnings:					
Information:					
18	NPL Documents	fin1_ref35.pdf	997207 94f6a0ec68380214f9259cf2056fecf1a855ddbfbf	no	6
Warnings:					
Information:					
19	NPL Documents	fin1_ref36.pdf	1585077 48a1512fd40d1abc87de22be5ca7c8e4196c5815	no	16
Warnings:					
Information:					

20	NPL Documents	fin1_ref37.pdf	1755953	no	13
			3d687971a467c6497c91e32ea751b9ed91347e9e		
Warnings:					
Information:					
Total Files Size (in bytes):				31515740	
<p>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.</p> <p><u>New Applications Under 35 U.S.C. 111</u> 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.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> 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.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> 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.</p>					

Electronic Acknowledgement Receipt	
EFS ID:	5637709
Application Number:	11370114
International Application Number:	
Confirmation Number:	1442
Title of Invention:	Method and system for protecting a computer and a network from hostile downloadables
First Named Inventor/Applicant Name:	Yigal Mordechai Edery
Customer Number:	74877
Filer:	Dawn-Marie Bey./Jeanne Paolella-Bald
Filer Authorized By:	Dawn-Marie Bey.
Attorney Docket Number:	FIN0001CON1CIP1CON2
Receipt Date:	02-JUL-2009
Filing Date:	07-MAR-2006
Time Stamp:	16:07:46
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	NPL Documents	fin1_ref38.pdf	465062 ef2e0aa2b692c88066e48943af3cb1fc3f1bb405	no	4

Warnings:

Information:

2	NPL Documents	fin1_ref39.pdf	1925165	no	9
			22366e4857185ac3abc6eb4f08ef22cbdfd298b1		
Warnings:					
Information:					
3	NPL Documents	fin1_ref40.pdf	1419632	no	7
			b4603956a4f7b2b64e7a9a02eba8d48d1343b028		
Warnings:					
Information:					
4	NPL Documents	fin1_ref41.pdf	1000440	no	5
			2926e77183fa99ac3f8412341f4d42364489ede		
Warnings:					
Information:					
5	NPL Documents	fin1_ref42a.pdf	18153278	no	163
			4f56ad3c508d806d08b317d1a497b06b1435ac55		
Warnings:					
Information:					
6	NPL Documents	fin1_ref42b.pdf	21217854	no	163
			0cc9a0fa2d27d3def3a8332a9675863580871f42		
Warnings:					
Information:					
Total Files Size (in bytes):			44181431		
<p>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.</p> <p><u>New Applications Under 35 U.S.C. 111</u> 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.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> 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.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> 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.</p>					



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

74877 7590 08/06/2009

King and Spalding LLP
1700 Pennsylvania Ave, NW
Suite 200
Washington, DC 20006

EXAMINER

REVAK, CHRISTOPHER A

ART UNIT

PAPER NUMBER

2431

DATE MAILED: 08/06/2009

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/370,114	03/07/2006	Yigal Mordechai Edery	FIN0001CON1CIP1CON2	1442

TITLE OF INVENTION: METHOD AND SYSTEM FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1510	\$300	\$0	\$1810	11/06/2009

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

74877 7590 08/06/2009

King and Spalding LLP
1700 Pennsylvania Ave, NW
Suite 200
Washington, DC 20006

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 (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

11/370,114 03/07/2006 Yigal Mordechai Edery FIN0001CON1CIP1CON2 1442

TITLE OF INVENTION: METHOD AND SYSTEM FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1510	\$300	\$0	\$1810	11/06/2009

EXAMINER	ART UNIT	CLASS-SUBCLASS
REVAK, CHRISTOPHER A	2431	726-022000

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, 1 _____
- (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 _____
- 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. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/370,114	03/07/2006	Yigal Mordechai Edery	FIN0001CON1CIP1CON2	1442
74877	7590	08/06/2009	EXAMINER	
King and Spalding LLP 1700 Pennsylvania Ave, NW Suite 200 Washington, DC 20006			REVAK, CHRISTOPHER A	
			ART UNIT	PAPER NUMBER
			2431	
DATE MAILED: 08/06/2009				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 659 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 659 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment 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 (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability	Application No.	Applicant(s)	
	11/370,114	EDERY ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2431	

-- 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 the response filed on 7/2/09.

2. ☒ The allowed claim(s) is/are 137,139,141,143 and 150-175.

3. ☐ 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.

4. ☐ 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.

5. ☐ 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).

6. ☐ 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. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) 2. <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) 3. <input checked="" type="checkbox"/> Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date <u>7/2/09</u> 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit of Biological Material	5. <input type="checkbox"/> Notice of Informal Patent Application 6. <input type="checkbox"/> Interview Summary (PTO-413), Paper No./Mail Date _____. 7. <input type="checkbox"/> Examiner's Amendment/Comment 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance 9. <input type="checkbox"/> Other _____.
--	---

/Christopher A. Revak/ Primary Examiner, Art Unit 2431	
---	--

NOTICE OF ALLOWANCE

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on July 2, is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.
2. The examiner notes that the information disclosure statement includes embedded hyperlinks which are not permissible, the examiner has deleted the portions containing those on the PTO form 1449. See MPEP § 608.01.

Terminal Disclaimer

3. The terminal disclaimer filed on June 5, 2009 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Allowable Subject Matter

4. Claims 137,139,141,143, and 150-175 are allowed.
5. The following is an examiner's statement of reasons for allowance:

It was not found to be taught in the prior art of receiving an incoming downloadable, performing a hashing function on the incoming downloadable to generate a downloadable ID. Security profile data is retrieved for the incoming downloadable from a database of downloadable security profiles indexed according to downloadable IDs based on the incoming downloadable ID, the security profile data

includes a list of suspicious operations that may be attempted by the downloadable. The representation of the retrieved downloadable security profile data is appended to the incoming downloadable to generate an appended downloadable and the appended downloadable is transmitted to a destination computer.

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."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Thursday, 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 517-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/Christopher A. Revak/
Primary Examiner, Art Unit 2431

Notice of References Cited	Application/Control No. 11/370,114	Applicant(s)/Patent Under Reexamination EDERY ET AL.	
	Examiner Christopher A. Revak	Art Unit 2431	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,093,135	08-2006	Radatti et al.	713/188
*	B	US-6,901,519	05-2005	Stewart et al.	726/24
	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	
	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.

Issue Classification 	Application/Control No. 11370114	Applicant(s)/Patent Under Reexamination EDERY ET AL.
	Examiner Christopher A Revak	Art Unit 2431

ORIGINAL						INTERNATIONAL CLASSIFICATION																	
CLASS		SUBCLASS				CLAIMED					NON-CLAIMED												
713		181				G	0	6	F	21 / 24 (2006.01.01)					G	0	6	F	21 / 24 (2006.01.01)				
CROSS REFERENCE(S)						G	0	6	F	11 / 30 (2006.01.01)					G	0	6	F	11 / 30 (2006.01.01)				
						H	0	4	L	9 / 00 (2006.01.01)					H	0	4	L	9 / 00 (2006.01.01)				
						G	0	6	F	15 / 16 (2006.01.01)					G	0	6	F	15 / 16 (2006.01.01)				
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																						
713	175	176																					
726	24																						

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant <input type="checkbox"/> CPA <input checked="" type="checkbox"/> T.D. <input type="checkbox"/> R.1.47															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	137	13	162												
8	139	14	163												
15	141	16	164												
22	143	17	165												
29	150	18	166												
30	151	19	167												
2	152	20	168												
3	153	21	169												
4	154	23	170												
5	155	24	171												
6	156	25	172												
7	157	26	173												
9	158	27	174												
10	159	28	175												
11	160														
12	161														

NONE		Total Claims Allowed:	
		30	
(Assistant Examiner)	(Date)		
/Christopher A Revak/ Primary Examiner Art Unit 2431	07/31/2009	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	11

Search Notes 	Application/Control No. 11370114	Applicant(s)/Patent Under Reexamination EDERY ET AL.
	Examiner Christopher A Revak	Art Unit 2431

SEARCHED			
Class	Subclass	Date	Examiner
none	none	2/16/09	CR

SEARCH NOTES		
Search Notes	Date	Examiner
PALM Inventor Name Search	2/16/09	CR
BRS Text Search: USPAT, US PGPUB, USOCR, DERWENT, FPRS, IBM TDB, EPO, JPO (see attached search strategy)	2/16/09; 7/30/09	CR
BRS Subclass Text Search: USPAT, US PGPUB (see attached search strategy)	2/16/09; 7/30/09	CR
DIALOG Text Search: COMPSCI, ELECTRON, SOFTWARE (see attached search strategy)	7/30/09	CR
Interference Search (see attached search strategy)	7/30/09	CR

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
713	168,175,176,179-181	7/30/09	CR
726	22-25	7/30/09	CR

--	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	318179	(code or executable or download\$5 or applet or java or javascript or script or activex) with(determin\$5 or ascertain\$3 or monitor\$3 or analy\$4 or inspect\$3 or examin\$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 14:01
L2	497520	(code or executable or download\$5 or applet or java or javascript or script or activex) with(append\$3 or attach\$4 or indicat\$3 or profile or character\$5 or identif\$7 or report\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 14:02
L3	89134	1 with 2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 14:03
L4	17450	(code or executable or download\$5 or applet or java or javascript or script or activex) with(hash\$3 or digest\$3 or (one adj2 way))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 14:05
L5	3669	4 with(index\$3 or id or identif\$7)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 14:06
L6	394	3 same 5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 14:06
L7	2743	5 with (append\$3 or attach\$4 or indicat\$3 or profile or character\$5 or identif\$7 or report\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 14:06
L8	390	6 same 7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 14:06

L9	4759	3 with(malicious or suspicious or attack\$3 or malware or virus or viral or trojan or worm or detail\$3 or list\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 14:07
L10	35	8 same 9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 14:08
L11	10696	(726/22-25 or 713/168,175,176,179-181). ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 14:09
L12	41	6 and 11	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 14:09

7/ 30/ 09 2:09:37 PM

C:\ Documents and Settings\ crevak\ My Documents\ EAST\ Workspaces\ default1.wsp

EAST Search History**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	10696	(726/22-25 or 713/168,175,176,179-181). ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 15:09
L2	3	("downloadable id").clm. and hash\$3.clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 15:10
L3	4	("downloadable id").clm. and 1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/30 15:10

7/ 30/ 09 3:10:54 PM**C:\ Documents and Settings\ crevak\ My Documents\ EAST\ Workspaces\ default1.wsp**

Receipt date: 07/02/2009

11370114 - GAU: 2431

Form PTO-1449 (Rev. 2-32)		U.S. Department of Commerce Patent & Trademark Office		Atty. Docket No. FIN0001-CON1-CIP1- CON2		Serial No. 11/370,114	
INFORMATION DISCLOSURE STATEMENT							
(Use several sheets if necessary)				Applicant Yigal Mordechai EDERY, et al.			
				Filing Date March 7, 2006		Group 2431	
U.S. PATENT DOCUMENTS							
Examiner Initial		Document Number	Date	Name	Class	Sub- Class	Filing Date (if appropriate)
		7,418,731	8/26/08	Touboul	726	22	5/3/04
		7,343,604	3/11/08	Grabarnik, et al.	719	313	7/25/03
		7,210,041	4/24/07	Gryaznov, et al.	713	188	4/30/01
		2005/0172338	8/4/05	Sandu, et al.	726	22	1/30/04
		2006/0031207	2/9/06	Bjarnestam, et al.	707	3	6/8/05
		6,917,953	7/12/05	Simon, et al.	707	204	12/17/01
		6,598,033	7/22/03	Ross, et al.	706	46	7/14/97
		6,519,679	2/11/03	Deviredy, et al.	711	114	6/11/99
		6,487,666	11/26/02	Shanklin, et al.	726	23	1/15/99
		6,434,669	8/13/02	Arimilli, et al.	711	128	9/7/99
		6,434,668	8/13/02	Arimilli, et al.	711	128	9/7/99
		2004/0088425	5/6/04	Rubinstein, et al.	709	230	10/31/02
		2004/0073811	4/15/04	Sanin	726	13	10/15/02
		6,425,058	7/23/02	Arimilli, et al.	711	134	9/7/99
		6,339,829	1/15/02	Beadle, et al.	726	15	7/30/98
		6,088,803	7/11/00	Tso, et al.	726	22	12/30/97
		6,088,801	7/11/00	Grecsek	726	1	1/10/97
U.S. PATENT DOCUMENTS CONT'D.							
EXAMINER /Christopher Revak/				DATE CONSIDERED 07/30/2009			
EXAMINER: Initial if citation 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.							

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /CR/

Serial No. 11/370,114 (Docket No. FIN0001-CON1-CIP1-CON2)
Information Disclosure Statement

Page 2 of 7

		5,987,611	11/16/99	Freund	726	4	5/6/97
		5,978,484	11/2/99	Apperson, et al.	705	54	4/25/96
		5,963,742	10/5/99	Williams	717	143	9/8/97
		5,956,481	9/21/99	Walsh, et al.	726	23	2/6/97
		5,951,698	9/14/99	Chen, et al.	714	38	10/2/96
		5,892,904	4/6/99	Atkinson, et al.	726	22	12/6/96
		5,884,033	3/16/99	Duvall, et al.	709	206	5/15/96
		5,881,151	3/9/99	Yamamoto	726	24	7/20/94
		5,864,683	1/26/99	Boebert, et al.	709	249	10/12/94
		5,859,966	1/12/99	Hayman, et al.	726	23	10/10/95
		5,850,559	12/15/98	Angelo, et al.	713	320	8/7/96
		5,832,274	11/3/98	Cutler, et al.	717	171	10/9/96
		5,832,208	11/3/98	Chen, et al.	726	24	9/5/96
		5,805,829	9/8/98	Cohen, et al.	709	202	10/1/96
		5,796,952	8/18/98	Davis, et al.	709	224	3/21/97
		5,784,459	7/21/98	Devarakonda, et al.	713	165	8/15/96
		5,765,205	6/9/98	Breslau, et al.	711	203	12/27/95
		5,761,421	6/2/98	van Hoff, et al.	709	223	3/25/96
		5,740,441	4/14/98	Yellin, et al.	717	134	12/20/95
		5,740,248	4/14/98	Fieres, et al.	713	156	12/19/96
		5,724,425	3/3/98	Chang, et al.	705	52	6/10/94
		5,720,033	2/17/98	Deo	726	2	7/25/95
		5,692,124	11/25/97	Holden, et al.	726	2	8/30/96
EXAMINER				DATE CONSIDERED			
/Christopher Revak/				07/30/2009			
EXAMINER: Initial if citation 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.							
U.S. PATENT DOCUMENTS CONT'D.							

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /CR/

Serial No. 11/370,114 (Docket No. FIN0001-CON1-CIP1-CON2)
Information Disclosure Statement

Page 3 of 7

		5,692,047	11/25/97	McManis	713	167	12/8/95
		5,675,711	10/7/97	Kephart, et al.	706	12	5/13/94
		5,638,446	6/10/97	Rubin	705	51	8/28/95
		5,579,509	11/26/96	Furtney, et al.	703	27	2/8/91
		5,572,643	11/5/96	Judson	709	218	10/19/95
		5,485,575	1/16/96	Chess, et al.	714	38	11/21/94
		5,485,409	1/16/96	Gupta, et al.	726	25	4/30/92
		5,414,833	5/9/95	Hershey, et al.	726	22	10/27/93
		5,361,359	11/1/94	Tajalli, et al.	726	23	8/31/92
		5,359,659	10/25/94	Rosenthal	726	24	10/19/92
		5,077,677	12/31/91	Murphy, et al.	706	62	6/12/89
FOREIGN PATENT DOCUMENTS							
		EP 1132796	9/12/01	Universite Catholique De Louvain	G06F	1/00	3/8/00
		EP 1091276	4/11/01	Alcatel	G06F	1/00	10/6/99
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)							
		Zhong, et al., "Security in the Large: is Java's Sandbox Scalable?," <i>Seventh IEEE Symposium on Reliable Distributed Systems</i> , pp. 1-6, October, 1998					
		Rubin, et al., "Mobile Code Security," <i>IEEE Internet</i> , pp. 30-34, December, 1998					
		Schmid, et al. "Protecting Data From Malicious Software," <i>Proceeding of the 18th Annual Computer Security Applications Conference</i> , pp. 1-10, 2002					
EXAMINER				DATE CONSIDERED			
/Christopher Revak/				07/30/2009			
EXAMINER: Initial if citation 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.							

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /CR/

Serial No. 11/370,114 (Docket No. FIN0001-CON1-CIP1-CON2)
Information Disclosure Statement

Page 4 of 7

OTHER DOCUMENTS CONT'D. (Including Author, Title, Date, Pertinent Pages, Etc.)	
	Corradi, et al., "A Flexible Access Control Service for Java Mobile Code," <i>IEEE</i> , pp. 356-365, 2000
	International Search Report for Application No. PCT/IB97/01626, 3 pp., May 14, 1998 (mailing date)
	International Search Report for Application No. PCT/IL05/00915, 4 pp., dated March 3, 2006
	Written Opinion for Application No. PCT/IL05/00915, 5 pp., dated March 3, 2006 (mailing date)
	International Search Report for Application No. PCT/IB01/01138, 4 pp., September 20, 2002 (mailing date)
	International Preliminary Examination Report for Application No. PCT/IB01/01138, 2 pp., dated December 19, 2002
	Gerzic, Amer, "Write Your Own Regular Expression Parser," November 17, 2003, 18 pp., Retrieved from the Internet: http://www.codeguru.com/Cpp/C++/cpp_info/parsing/article.php/c4092/
	Power, James, "Lexical Analysis," 4 pp., May 14, 2006, Retrieved from the Internet: http://www.cs.may.ie/~jpower/Courses/compilers/notes/lexical.pdf
	Sitaker, Kragen, "Rapid Genetic Evolution of Regular Expressions" [online], <i>The Mail Archive</i> , April 24, 2004 (retrieved on December 7, 2004), 5 pp., Retrieved from the Internet: http://www.mail-archive.com/kragen-bol@canonical.org/msg00097.html
	"Lexical Analysis: DFA Minimization & Wrap Up" [online], Fall, 2004 [retrieved on March 2, 2005], 8 pp., Retrieved from the Internet: http://www.cwi.nl/~ice/cwi/comp112/lecture/L06LexWrapUp4.pdf
	"Minimization of DFA" [online], [retrieved on December 7, 2004], 7 pp., Retrieved from the Internet: http://www.cs.odu.edu/~toleda/neric/396/techd/regular/fatmin/fatmin.html
EXAMINER	/Christopher Revak/
DATE CONSIDERED	07/30/2009
EXAMINER: Initial if citation 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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /CR/

Serial No. 11/370,114 (Docket No. FIN0001-CON1-CIP1-CON2)
Information Disclosure Statement

Page 5 of 7

OTHER DOCUMENTS CONT'D. (Including Author, Title, Date, Pertinent Pages, Etc.)	
	"Algorithm: NFS -> DFA" [online], Copyright 1999-2001 [retrieved on December 7, 2004], 4 pp., Retrieved from the Internet: http://lav4.cs.miami.edu/garinal/CANFA/page16.html
	"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/~hansen/classes/3813fall01/slides/OGMinimize.pdf
	Watson, Bruce W., "Constructing Minimal Acyclic Deterministic Finite Automata," [retrieved on March 20, 2005], 38 pp., Retrieved from the Internet: http://www.wintec.nz/~watson/2F870/downloads/modfs_dfs.pdf
	Chang, Chia-Hsiang, "From Regular Expressions to DFA's Using Compressed NFA's," October, 1992, 243 pp., http://www.csrcr.edu/web/Research/Theses/chang_chia-hsiang.pdf
	"Products," Articles published on the Internet, "Revolutionary Security for a New Computing Paradigm" regarding SurfinGate™, 7 pp. no date provided
	"Release Notes for the Microsoft ActiveX Development Kit," August 13, 1996, activex.adsp.or.jp/metsdk/readme.txt , pp. 1-10
	Doyle, et al., "Microsoft Press Computer Dictionary," Microsoft Press, 2d Edition, pp. 137-138, 1993
	Finjan Software Ltd., "Powerful PC Security for the New World of Java™ and Downloadables, Surfin Shield™," Article published on the Internet by Finjan Software Ltd., 2 pp. 1996
	Finjan Software Ltd., "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
	Finjan Software Ltd., "Finjan Announces Major Power Boost and New Features for SurfinShield™ 2.0," Las Vegas Convention Center/Pavillion 5 P5551, 3 pp., November 18, 1996
EXAMINER	/Christopher Revak/
DATE CONSIDERED	07/30/2009
EXAMINER: Initial if citation 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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /CR/

Serial No. 11/370,114 (Docket No. FIN0001-CON1-CIP1-CON2)
Information Disclosure Statement

Page 6 of 7

OTHER DOCUMENTS CONT'D. (Including Author, Title, Date, Pertinent Pages, Etc.)	
	Finjan Software Ltd., "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
	Finjan Software Ltd., "Java Security: Issues & Solutions," Article published on the Internet by Finjan Software Ltd., 8 pp. 1996
	Finjan Software Ltd., Company Profile, "Finjan - Safe Surfing, The Java Security Solutions Provider," Article published on the Internet by Finjan Software Ltd., 3 pp., October 31, 1996
	"IBM AntiVirus User's Guide, Version 2.4," International Business Machines Corporation, pp. 6-7, November 15, 1995
	Khare, R., "Microsoft Authenticode Analyzed" [online], July 22, 1996 [retrieved on June 25, 2003], 2 pp., Retrieved from the Internet: http://www.xent.com/FORK-archive/smmr96/0338.html
	LaDue, M., "Online Business Consultant: Java Security: Whose Business is It?, Article published on the Internet, Home Page Press, Inc., 4 pp., 1996
	Leach, Norvin, et al., "IE 3.0 Applets Will Earn Certification," <i>PC Week</i> , Vol. 13, No. 29, 2 pp., July 22, 1996
	Moritz, R., "Why We Shouldn't Fear Java," <i>Java Report</i> , pp. 51-56, February, 1997
	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/metsdk/help/overview.htm
	Microsoft® Authenticode Technology, "Ensuring Accountability and Authenticity for Software Components on the Internet," Microsoft Corporation, October, 1996, including Abstract, Contents, Introduction, and pp. 1-10
	Microsoft Corporation, Web Page Article "Frequently Asked Questions About Authenticode," last updated February 17, 1997, printed December 23, 1998, URL: http://www.microsoft.com/windows/security/authenticode/faq.asp , pp. 1-13
EXAMINER	DATE CONSIDERED
/Christopher Revak/	07/30/2009
EXAMINER: Initial if citation 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.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /CR/

Serial No. 11/370,114 (Docket No. FIN0001-CON1-CIP1-CON2)
Information Disclosure Statement

Page 7 of 7

OTHER DOCUMENTS CONT'D. (Including Author, Title, Date, Pertinent Pages, Etc.)	
	Okamoto, E., et al., "ID-Based Authentication System for Computer Virus Detection," <i>IEEE/IEE Electronic Library online, Electronics Letters</i> , Vol. 26, Issue 15, ISSN 0013-5194, July 19, 1990, Abstract and pp. 1169-1170, URL: http://ieeexplore.ieee.org/abstract/abstract/2431/2431ViewTemplate?docview=54662431
	Omura, J. K., "Novel Applications of Cryptography in Digital Communications," <i>IEEE Communications Magazine</i> , pp. 21-29, May, 1990
	Schmitt, D.A., ".EXE files, OS-2 style," <i>PC Tech Journal</i> , Vol. 6, No. 11, p. 76(13), November, 1988
	Zhang, X. N., "Secure Code Distribution," <i>IEEE/IEE Electronic Library online, Computer</i> , Vol. 30, Issue 6, pp. 76-79, June, 1997
	D. Grune, et al., "Parsing Techniques: A Practical Guide," John Wiley & Sons, Inc., New York, New York, USA, pp. 1-326, 2000
EXAMINER /Christopher Revak/ DATE CONSIDERED 07/30/2009	
EXAMINER: Initial if citation 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.	

15157/105016
 Doc. No. 1212219

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /CR/

? show files

File 2:INSPEC 1898-2009/Jul W3
(c) 2009 The IET

File 6:NTIS 1964-2009/Aug W2
(c) 2009 NTIS, Intl Cpyrght All Rights Res

File 8:Ei Compendex(R) 1884-2009/Jul W3
(c) 2009 Elsevier Eng. Info. Inc.

File 34:SciSearch(R) Cited Ref Sci 1990-2009/Jul W3
(c) 2009 The Thomson Corp

File 35:Dissertation Abs Online 1861-2009/Jun
(c) 2009 ProQuest Info&Learning

File 56:Computer and Information Systems Abstracts 1966-2009/Jul
(c) 2009 CSA.

File 60:ANTE: Abstracts in New Tech & Engineer 1966-2009/Jul
(c) 2009 CSA.

File 65:Inside Conferences 1993-2009/Jul 30
(c) 2009 BLDSC all rts. reserv.

File 92:IHS Intl.Stds.& Specs. 1999/Nov
(c) 1999 Information Handling Services

File 95:TEME-Technology & Management 1989-2009/Jul W1
(c) 2009 FIZ TECHNIK

File 99:Wilson Appl. Sci & Tech Abs 1983-2009/Jun
(c) 2009 The HW Wilson Co.

File 103:Energy SciTec 1974-2009/Jul B1
(c) 2009 Contains copyrighted material

File 144:Pascal 1973-2009/Jul W4
(c) 2009 INIST/CNRS

File 239:Mathsci 1940-2009/Aug
(c) 2009 American Mathematical Society

File 275:Gale Group Computer DB(TM) 1983-2009/Jul 01
(c) 2009 Gale/Cengage

File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
(c) 2006 The Thomson Corp

File 647:UBM Computer Fulltext 1988-2009/Jul W4
(c) 2009 UBM, LLC

File 674:Computer News Fulltext 1989-2006/Sep W1
(c) 2006 IDG Communications

File 696:DIALOG Telecom. Newsletters 1995-2009/Jul 29
(c) 2009 Dialog

File 9:Business & Industry(R) Jul/1994-2009/Jul 29
(c) 2009 Gale/Cengage

File 15:ABI/Inform(R) 1971-2009/Jul 29
(c) 2009 ProQuest Info&Learning

File 16:Gale Group PROMT(R) 1990-2009/Jul 07
(c) 2009 Gale/Cengage

File 18:Gale Group F&S Index(R) 1988-2009/Jul 07
(c) 2009 Gale/Cengage

File 20:Dialog Global Reporter 1997-2009/Jul 30
(c) 2009 Dialog

File 36:MetalBase 1965-20090730
(c) 2009 The Thomson Corporation

File 80:TGG Aerospace/Def.Mkts(R) 1982-2009/Jul 03
(c) 2009 Gale/Cengage

File 148:Gale Group Trade & Industry DB 1976-2009/Jul 14
(c) 2009 Gale/Cengage

File 160:Gale Group PROMT(R) 1972-1989
(c) 1999 The Gale Group

File 256:TecTrends 1982-2009/Jul W4
(c) 2009 Info.Sources Inc. All rights res.

File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
(c) 2002 Gale/Cengage

File 621:Gale Group New Prod.Annou.(R) 1985-2009/Jun 23
(c) 2009 Gale/Cengage
File 624:McGraw-Hill Publications 1985-2009/Jul 30
(c) 2009 McGraw-Hill Co. Inc
File 635:Business Dateline(R) 1985-2009/Jul 30
(c) 2009 ProQuest Info&Learning
File 636:Gale Group Newsletter DB(TM) 1987-2009/Jul 07
(c) 2009 Gale/Cengage
? ds

Set	Items	Description
S1	453683	(CODE OR EXECUTABLE OR DOWNLOAD????? OR APPLET OR JAVA OR - JAVASCRIPT OR ACTIVEX OR SCRIPT)(16N)(DETERMIN????? OR ASCERT- AIN??? OR MONITOR??? OR ANALY????? OR INSPECT??? OR EXAMIN????- ?)
S2	492282	(CODE OR EXECUTABLE OR DOWNLOAD????? OR APPLET OR JAVA OR - JAVASCRIPT OR ACTIVEX OR SCRIPT)(16N)(APPEND??? OR ATTACH???? OR INDICAT??? OR PROFILE OR CHARACTER????? OR IDENTIF??????? - OR REPORT???)
S3	44206	S1(16N)S2
S4	9627	(CODE OR EXECUTABLE OR DOWNLOAD????? OR APPLET OR JAVA OR - JAVASCRIPT OR ACTIVEX OR SCRIPT)(16N)(HASH??? OR DIGEST??? OR (ONE(2W)WAY))
S5	296	S4(16N)(INDEX??? OR ID OR IDENTIF?????????)
S6	20	S3(S)S5
?		

FIN0001-CON1-CIP1-CON2

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Yigal Mordechai EDERY, et al.

Group Art Unit: 2431

Serial No. : 11/370,114

Examiner: Christopher A. Revak

Filed: March 7, 2006

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

SUBMISSION OF ISSUE FEE PAYMENT

U.S. Patent and Trademark Office
Customer Service Window, Mail Stop Issue Fee
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

Responsive to the Notice of Allowance and Issue Fee Due mailed August 6, 2009, the undersigned is submitting herewith the Issue Fee in the amount of \$1,810.00 in the above-identified application. A copy of Part B of the issue fee transmittal is submitted herewith. Please address all future correspondence in this application to the undersigned at the following address:

Dawn-Marie Bey
KING & SPALDING LLP
1700 Pennsylvania Avenue, N.W.
Suite 200
Washington, DC 20006
(202) 737-0500

Serial No. 11/370,114

2

Docket No. FIN0001-CON1-CIP1-CON2

This application is assigned to Finjan Software, Ltd., Hamachshev St. 1, New Industrial Area, Netanya, Israel, 42504.

The Commissioner is hereby authorized to charge any additional fees associated with this communication or credit any overpayment to Deposit Account No. 50-4402.

Entry of this submission and prompt notification thereof is respectfully requested.

Respectfully submitted,

Dated: 9-24-09

KING & SPALDING LLP
1700 Pennsylvania Avenue, N.W.
Suite 200
Washington, DC 20006
(202) 737-0500

By: /Dawn-Marie Bey - 44,442/
Dawn-Marie Bey
Registration No. 44,442

15157/105016
Doc. No. 1342267

PART B - FEE(S) TRANSMITTAL

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

74877 7590 08/06/2009

King and Spalding LLP
1700 Pennsylvania Ave, NW
Suite 200
Washington, DC 20006

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 (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

11/370,114 03/07/2006 Yigal Mordechai Edery FIN0001CON1CIP1CON2 1442

TITLE OF INVENTION: METHOD AND SYSTEM FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1510	\$300	\$0	\$1810	11/06/2009

EXAMINER	ART UNIT	CLASS-SUBCLASS
REVAK, CHRISTOPHER A	2431	726-022000

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 King & Spalding LLP
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. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

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 submitted:

- ☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
☒ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 50-4402 (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Dawn-Marie Bey/

Date 9-24-09

Typed or printed name Dawn-Marie Bey

Registration No. 44,442

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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

Electronic Patent Application Fee Transmittal				
Application Number:		11370114		
Filing Date:		07-Mar-2006		
Title of Invention:		METHOD AND SYSTEM FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES		
First Named Inventor/Applicant Name:		Yigal Mordechai Edery		
Filer:		Dawn-Marie Bey./Jeanne Paoletta-Bald		
Attorney Docket Number:		FIN0001CON1CIP1CON2		
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:				
Utility Appl issue fee	1501	1	1510	1510
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1810

Electronic Acknowledgement Receipt	
EFS ID:	6137682
Application Number:	11370114
International Application Number:	
Confirmation Number:	1442
Title of Invention:	METHOD AND SYSTEM FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES
First Named Inventor/Applicant Name:	Yigal Mordechai Edery
Customer Number:	74877
Filer:	Dawn-Marie Bey./Jeanne Paolella-Bald
Filer Authorized By:	Dawn-Marie Bey.
Attorney Docket Number:	FIN0001CON1CIP1CON2
Receipt Date:	24-SEP-2009
Filing Date:	07-MAR-2006
Time Stamp:	14:00:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$1810
RAM confirmation Number	192
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	----------------------------------	------------------	------------------

1	Issue Fee Payment (PTO-85B)	fin0001con1cip1con2_issfeetrans.pdf	84907 f974cdde2f0d220334a88d7728bd56fac91d6e5d	no	2
Warnings:					
Information:					
2	Issue Fee Payment (PTO-85B)	fin0001con1cip1con2_partb.pdf	187414 79264d09072512c6e5662b9822fb1215f0797567	no	1
Warnings:					
Information:					
3	Fee Worksheet (PTO-875)	fee-info.pdf	32193 3968552453ef55d6420688104c7fb0b72b57d0a1	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			304514		
<p>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.</p> <p><u>New Applications Under 35 U.S.C. 111</u> 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.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> 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.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> 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.</p>					



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.
11/370,114	11/03/2009	7613926	FIN0001CON1CIP1CON2	1442

74877 7590 10/14/2009
King and Spalding LLP
1700 Pennsylvania Ave, NW
Suite 200
Washington, DC 20006

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 659 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment 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 (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Yigal Mordechai Edery, Pardesia, ISRAEL;
Nimrod Itzhak Vered, Goosh Tel-Mond, ISRAEL;
David R. Kroll, San Jose, CA;
Shlomo Touboul, Kefar-Haim, ISRAEL;



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
11/370,114	7613926	2431	9200



Correspondence Address/Fee Address Change

The following fields have been set to Customer Number 115222 on 05/20/2013

- Correspondence Address
- Maintenance Fee Address

The address of record for Customer Number 115222 is:

115222
Bey & Cotropia PLLC
213 Bayly Court
Richmond, VA 23229

AO 120 (Rev. 2/99)

TO: Mail Stop 8 Director of the U.S. Patent & Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been
filed in the U.S. District Court Northern District California on the ☒ Patents or ☐ Trademarks:

DOCKET NO. CV 14-01197 JCS	DATE FILED 3/14/14	U.S. DISTRICT COURT 450 Golden Gate Avenue, 16th Floor, San Francisco CA 94102
PLAINTIFF FINJAN INC		DEFENDANT SOPHOS INC
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,804,780		***see Attach Complaint***
2 8,141,154		
3 7,613,918		
4 7,757,289		
5		

In the above—entitled case, the following patent(s) have been included:

DATE INCLUDED	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading		
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK	
1 7,613,926			
2 6,154,844			
3			
4			
5			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT		
CLERK Richard W. Wicking	(BY) DEPUTY CLERK Gina Agustine	DATE March 15, 2014

Copy 1—Upon initiation of action, mail this copy to Commissioner Copy 3—Upon termination of action, mail this copy to Commissioner
Copy 2—Upon filing document adding patent(s), mail this copy to Commissioner Copy 4—Case file copy

also conduct cloud-based selective sandboxing to analyze suspicious content with both web protection and intrusion prevention. The following shows the cloud based sandboxing features:

Advanced Threat Protection Options

☒ Send suspicious content to SophosLabs for analysis

SophosLabs features a cloud-based sandbox where the behavior of suspected malware can be automatically observed and analysed. This helps ensure speedy delivery of protection updates directly to your UTM. Disabling this functionality may increase defense response time.

All submissions are sent over a secure channel and are handled according to the [SophosLabs Information Security Policy](#).

☒ Apply

Cloud-based selective sandboxing allows SophosLabs to analyze suspicious content.

See <http://blogs.sophos.com/2014/02/26/whats-coming-in-sophos-utm-accelerated-9-2-5-advanced-threat-protection-atp/>, a true and correct copy of which is attached hereto as Exhibit H.

32. Sophos WebLENS technology blocks threats using content reassembly with JavaScript emulation and behavioral analysis. Its purpose is to stop malicious code at the network layer before it is passed to the browser.

SOPHOS' INFRINGEMENT OF FINJAN'S PATENTS

33. Defendant has been and is now infringing the '780 Patent, the '154 Patent, the '918 Patent, the '289 Patent, the '926 Patent, and the '844 Patent (collectively "the Patents-In-Suit") in this judicial District, and elsewhere in the United States by, among other things, making, using, importing, selling, and/or offering for sale the claimed system and methods that utilize Sophos Live Protection, Advanced Threat Protection, and WebLENS, including without limitation on Enduser Protection Suites, Endpoint Antivirus, Endpoint Antivirus Cloud, Sophos Cloud, Unified Threat Management, Next-Gen Firewall, Secure Web Gateway, Secure Email Gateway, and Server Security.

(Direct Infringement of the '780 Patent pursuant to 35 U.S.C. § 271(a))

36. Defendant has infringed and continues to infringe one or more claims of the '780 Patent in violation of 35 U.S.C. § 271(a).

37. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

38. Defendant's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

39. Defendant's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant's products and services, including but not limited to Sophos Live Protection, which embodies the patented invention of the '780 Patent.

40. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

41. Defendant's infringement of the '780 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

COUNT II

(Indirect Infringement of the '780 Patent pursuant to 35 U.S.C. § 271(b))

42. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

43. Defendant has induced and continues to induce infringement of at least claims 1-8 of the '780 Patent under 35 U.S.C. § 271(b).

44. In addition to directly infringing the '780 Patent, Defendant indirectly infringes the '780 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including but not limited to its customers, users and developers, to perform some of the steps of the method claims, either literally or under the doctrine of equivalents, of the '780 Patent, where all the steps of the method claims are performed by either Sophos or its customers, users or developers, or some combination thereof. Defendant knew or was willfully blind to the fact that it was inducing others, including customers, users and developers, to infringe by practicing, either themselves or in conjunction with Defendant, one or more method claims of the '780 Patent.

45. Defendant knowingly and actively aided and abetted the direct infringement of the '780 Patent by instructing and encouraging its customers, users and developers to use the Sophos Live Protection. Such instructions and encouragement include but are not limited to, advising third parties to use the Sophos Live Protection in an infringing manner, providing a mechanism through which third parties may infringe the '780 Patent, specifically through the use of the Sophos Live Protection, advertising and promoting the use of the Sophos Live Protection in an infringing manner, and distributing guidelines and instructions to third parties on how to use the Sophos Live Protection in an infringing manner.

1 46. Sophos regularly updates and maintains the Sophos Support/Labs to provide
2 demonstration, instructions, and technical assistance to users to help them use the Sophos Live
3 Protection, including:

- 4 • Providing an overview of how Live Protections works. *See* [http://www.sophos.com/en-](http://www.sophos.com/en-us/support/knowledgebase/111334.aspx)
5 [us/support/knowledgebase/111334.aspx](http://www.sophos.com/en-us/support/knowledgebase/111334.aspx), a true and correct copy of which is attached hereto as
6 Exhibit I;
- 7 • Giving step-by-step instructions on how to turn Live Protection on and off, combined with a
8 video demonstration of the functionalities of Live Protection. *See* [http://www.sophos.com/en-](http://www.sophos.com/en-us/support/knowledgebase/116371.aspx)
9 [us/support/knowledgebase/116371.aspx](http://www.sophos.com/en-us/support/knowledgebase/116371.aspx), a true and correct copy of which is attached hereto as
10 Exhibit J;
- 11 • Maintaining a list of behavior profiles such as SUS/ZelXor-A, created by Sophos' labs and
12 posted on Sophos' website for download. *See* [http://www.sophos.com/en-us/threat-](http://www.sophos.com/en-us/threat-center/threat-analyses/suspicious-behavior-and-files/Sus~ZelXor-A.aspx)
13 [center/threat-analyses/suspicious-behavior-and-files/Sus~ZelXor-A.aspx](http://www.sophos.com/en-us/threat-center/threat-analyses/suspicious-behavior-and-files/Sus~ZelXor-A.aspx), a true and correct
14 copy of which is attached hereto as Exhibit K;
- 15 • Maintaining a list of Live Protection errors and suggesting ways of resolving them. *See*
16 <http://www.sophos.com/en-us/support/knowledgebase/111244.aspx>, a true and correct copy of
17 which is attached hereto as Exhibit L.

18 47. Sophos provides quick start guides, administration guides, user guides, and operating
19 instructions which cover in depth aspects of operating Sophos offerings. *See*
20 <https://www.sophos.com/en-us/support/documentation.aspx>, a true and correct copy of which is
21 attached hereto as Exhibit M.

22 48. Sophos maintains and updates a YouTube channel where training and informational
23 videos are posted in order to promote the use of Sophos products. *See*
24 <http://www.youtube.com/user/SophosGlobalSupport?feature=watch>, a true and correct copy of which
25 is attached hereto as Exhibit N.

26 49. Sophos maintains and promotes the Sophos Partner Program to encourage and expand
27 use of the Sophos Live Protection by offering up-to-date training and certification enabled by a full
28 curriculum of courses in order to increase skills and competency. *See* [http://www.sophos.com/en-](http://www.sophos.com/en-us/partners.aspx)
[us/partners.aspx](http://www.sophos.com/en-us/partners.aspx), a true and correct copy of which is attached hereto as Exhibit O; *see also*

1 <http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos-partnership-with-sophos-na.pdf>, a
2 true and correct copy of which is attached hereto as Exhibit P.

3 50. Sophos maintains and promotes the Sophos Managed Service Provider program in
4 which Sophos trains IT personnel to support Sophos products. See [http://www.sophos.com/en-](http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf)
5 [us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf](http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf), a true and correct copy of
6 which is attached hereto as Exhibit Q.

7 51. Sophos provides Global System Integrators who provide advisory, solution and deliver
8 services to its customers across all market sections. These services include consulting, systems
9 integration, managed services and full facilities outsourcing. See [http://www.sophos.com/en-](http://www.sophos.com/en-us/partners/global-system-integrators.aspx)
10 [us/partners/global-system-integrators.aspx](http://www.sophos.com/en-us/partners/global-system-integrators.aspx), a true and correct copy of which is attached hereto as
11 Exhibit R.

12 52. Sophos maintains and offers Sophos Professional Services. Sophos Professional
13 Services plans the requirements of a client security needs, builds the endpoint and network solutions
14 for the clients, and then manages the Sophos implemented solutions. See [http://www.sophos.com/en-](http://www.sophos.com/en-us/medialibrary/PDFs/professionalservices/sophosprofessionalservicesbrna.pdf)
15 [us/medialibrary/PDFs/professionalservices/sophosprofessionalservicesbrna.pdf](http://www.sophos.com/en-us/medialibrary/PDFs/professionalservices/sophosprofessionalservicesbrna.pdf), a true and correct
16 copy of which is attached hereto as Exhibit S.

17 53. Defendant has had knowledge of the '780 Patent at least as of the time it learned of
18 this action for infringement and by continuing the actions described above, has had the specific intent
19 to or was willfully blind to the fact that its actions would induce infringement of the '780 Patent.

20 54. Sophos actively and intentionally maintains websites, including Sophos' Support, to
21 promote the Sophos Live Protection and to encourage potential customers, users and developers to
22 use the Sophos Live Protection in the manner described by Finjan.
23
24
25
26
27
28

1 55. Sophos actively updates websites, including Sophos' Support, to promote the Sophos
2 Live Protection and Advanced Threat Protection, including the Sophos Unified Threat Management,
3 Next Generation Firewall, Secure Web Gateway, Secure E-mail Gateway, Sophos Cloud, Endpoint
4 Antivirus Cloud, Endpoint Antivirus, Enduser Protection Suites, and Server Security, to encourage
5 users and developers to practice the methods taught in the '780 Patent.

6
7 **COUNT III**
8 **(Direct Infringement of the '154 Patent pursuant to 35 U.S.C. § 271(a))**

9 56. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the
10 allegations of the preceding paragraphs, as set forth above.

11 57. Defendant has infringed and continues to infringe one or more claims of the '154
12 Patent in violation of 35 U.S.C. § 271(a).

13 58. Defendant's infringement is based upon literal infringement or, in the alternative,
14 infringement under the doctrine of equivalents.

15 59. Defendant's acts of making, using, importing, selling, and/or offering for sale infringing
16 products and services have been without the permission, consent, authorization or license of Finjan.

17 60. Defendant's infringement includes, but is not limited to, the manufacture, use, sale,
18 importation and/or offer for sale of Defendant's products and services, including but not limited to
19 Sophos Live Protection and Sophos Advanced Threat Protection, which embody the patented
20 invention of the '154 Patent.

21
22 61. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to
23 suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled
24 to preliminary and/or permanent injunctive relief.

25 62. Defendant's infringement of the '154 Patent has injured and continues to injure Finjan
26 in an amount to be proven at trial.
27
28

COUNT IV

(Direct Infringement of the '918 Patent pursuant to 35 U.S.C. § 271(a))

63. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

64. Defendant has infringed and continues to infringe one or more claims of the '918 Patent in violation of 35 U.S.C. § 271(a).

65. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

66. Defendant's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

67. Defendant's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant's products and services, including but not limited to Sophos Live Protection and Sophos Advanced Threat Protection, which embodies the patented invention of the '918 Patent.

68. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

69. Defendant's infringement of the '918 Patent has injured and continues to injure Finjan in an amount to be proven at trial.

COUNT V

(Indirect Infringement of the '918 Patent pursuant to 35 U.S.C. § 271(b))

70. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

71. Defendant has induced and continues to induce infringement of at least claims 1-11, 22-27, and 34 of the '918 Patent under 35 U.S.C. § 271(b).

1 72. In addition to directly infringing the '918 Patent, Defendant indirectly infringes the
2 '918 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including
3 but not limited to its customers, users and developers, to perform some of the steps of the method
4 claims, either literally or under the doctrine of equivalents, of the '918 Patent, where all the steps of
5 the method claims are performed by either Sophos or its customers, users or developers, or some
6 combination thereof. Defendant knew or was willfully blind to the fact that it was inducing others,
7 including customers, users and developers, to infringe by practicing, either themselves or in
8 conjunction with Defendant, one or more method claims of the '918 Patent.
9

10 73. Defendant knowingly and actively aided and abetted the direct infringement of the
11 '918 Patent by instructing and encouraging its customers, users and developers to use Sophos Live
12 Protection and Sophos Advanced Threat Protection. Such instructions and encouragement include
13 but are not limited to, advising third parties to use the Sophos Live Protection and Sophos Advanced
14 Threat Protection in an infringing manner, providing a mechanism through which third parties may
15 infringe the '918 Patent, specifically through the use of the Sophos Live Protection and Sophos
16 Advanced Threat Protection, advertising and promoting the use of the Sophos Live Protection and
17 Sophos Advanced Threat Protection in an infringing manner, and distributing guidelines and
18 instructions to third parties on how to use the Sophos Live Protection and Sophos Advanced Threat
19 Protection in an infringing manner.
20

21 74. Sophos regularly updates and maintains the Sophos Support/Labs to provide
22 demonstration, instructions, and technical assistance to users to help them use the Sophos Live
23 Protection and Advanced Threat Protection, including:
24

- 25 • Providing an overview of how Live Protections works. *See* <http://www.sophos.com/en-us/support/knowledgebase/111334.aspx>, a true and correct copy of which is attached hereto as
26 Exhibit I;
27
28

- 1 • Giving step-by-step instructions on how to turn Live Protection on and off, combined with a
2 video demonstration of the functionalities of Live Protection. See <http://www.sophos.com/en-us/support/knowledgebase/116371.aspx>, a true and correct copy of which is attached hereto as
3 Exhibit J;
- 4 • Maintaining a list of behavior profiles such as SUS/ZelXor-A, created by Sophos' labs and
5 posted on Sophos' website for download. See <http://www.sophos.com/en-us/threat-center/threat-analyses/suspicious-behavior-and-files/Sus~ZelXor-A.aspx>, a true and correct
6 copy of which is attached hereto as Exhibit T;
- 7 • Maintaining a list of Live Protection errors and suggesting ways of resolving them. See
8 <http://www.sophos.com/en-us/support/knowledgebase/111244.aspx>, a true and correct copy of
9 which is attached hereto as Exhibit L;
- 10 • Describing what Advanced Threat Protection is used for and how to adjust its settings. See
11 <http://blogs.sophos.com/2014/02/26/whats-coming-in-sophos-utm-accelerated-9-2-5-advanced-threat-protection-atp/>, a true and correct copy of which is attached hereto as Exhibit H.
- 12 • Providing a YouTube video on the new feature of Advanced Threat Protection. Available at
13 <http://www.youtube.com/watch?v=qcGV-R1z6io> (last visited March 13, 2014);
- 14 • Providing a written "how to" configure the Advanced Threat Protection. See
15 <http://www.sophos.com/en-us/support/knowledgebase/120330.aspx>, a true and correct copy of
16 which is attached hereto as Exhibit U.

17 75. Sophos provides quick start guides, administration guides, user guides, and operating
18 instructions which cover in depth aspects of operating Sophos offerings. See
19 <https://www.sophos.com/en-us/support/documentation.aspx>, a true and correct copy of which is
20 attached hereto as Exhibit M.

21 76. Sophos maintains and updates a YouTube channel where training and informational
22 videos are posted in order to promote the use of Sophos products. See
23 <http://www.youtube.com/user/SophosGlobalSupport?feature=watch>, a true and correct copy of which
24 is attached hereto as Exhibit N.

25 77. Sophos maintains and promotes the Sophos Partner Program to encourage and expand
26 use of the Sophos Live Protection by offering up-to-date training and certification enabled by a full
27 curriculum of courses in order to increase skills and competency. See <http://www.sophos.com/en->
28

1 [us/partners.aspx](#), a true and correct copy of which is attached hereto as Exhibit O; *see also*
2 <http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos-partnership-with-sophos-na.pdf>, a
3 true and correct copy of which is attached hereto as Exhibit P.

4 78. Sophos maintains and promotes the Sophos Managed Service Provider program in
5 which Sophos trains IT personnel to support Sophos products. *See* [http://www.sophos.com/en-](http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf)
6 [us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf](http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf), a true and correct copy of
7 which is attached hereto as Exhibit Q.

8 79. Sophos provides Global System Integrators who provide advisory, solution and deliver
9 services to its customers across all market sections. These services include consulting, systems
10 integration, managed services and full facilities outsourcing. *See* [http://www.sophos.com/en-](http://www.sophos.com/en-us/partners/global-system-integrators.aspx)
11 [us/partners/global-system-integrators.aspx](http://www.sophos.com/en-us/partners/global-system-integrators.aspx), a true and correct copy of which is attached hereto as
12 Exhibit R.

13 80. Sophos maintains and offers Sophos Professional Services. Sophos Professional
14 Services plans the requirements of a client security needs, builds the endpoint and network solutions
15 for the clients, and then manages the Sophos implemented solutions. *See* [http://www.sophos.com/en-](http://www.sophos.com/en-us/medialibrary/PDFs/professionalservices/sophosprofessionalservicesbrna.pdf)
16 [us/medialibrary/PDFs/professionalservices/sophosprofessionalservicesbrna.pdf](http://www.sophos.com/en-us/medialibrary/PDFs/professionalservices/sophosprofessionalservicesbrna.pdf), a true and correct
17 copy of which is attached hereto as Exhibit S.

18 81. Defendant has had knowledge of the '918 Patent at least as of the time it learned of
19 this action for infringement and by continuing the actions described above has had the specific intent
20 to or was willfully blind to the fact that its actions would induce infringement of the '918 Patent.

21 82. Sophos actively and intentionally maintains websites, including Sophos' Support, to
22 promote the Sophos Live Protection and Advanced Threat Protection and to encourage potential users
23
24
25
26
27
28

1 PAUL J. ANDRE (State Bar No. 196585)
pandre@kramerlevin.com
2 LISA KOBIALKA (State Bar No. 191404)
lkobialka@kramerlevin.com
3 JAMES HANNAH (State Bar No. 237978)
jhannah@kramerlevin.com
4 KRAMER LEVIN NAFTALIS & FRANKEL LLP
990 Marsh Road
5 Menlo Park, CA 94025
Telephone: (650) 752-1700
6 Facsimile: (650) 752-1800
7 *Attorneys for Plaintiff*
8 FINJAN, INC.

ECF DOCUMENT
I hereby attest and certify this is a printed copy of a
document which was electronically filed with the United States
District Court for the Northern District of California.
Date Filed: 3/14/14
RICHARD W. WIEKING, Clerk
By: GINA AGUSTINE, Deputy Clerk

9
10 **IN THE UNITED STATES DISTRICT COURT**
11 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

12
13 FINJAN, INC., a Delaware Corporation,
14 Plaintiff,

15 v.

16 SOPHOS, INC., a Massachusetts Corporation,
17 Defendant.

Case No.:

C14-1197JCS

**COMPLAINT FOR PATENT
INFRINGEMENT**

DEMAND FOR JURY TRIAL

18
19
20
21
22
23
24
25
26
27
28
COMPLAINT FOR PATENT INFRINGEMENT

1 and developers to use the Sophos Live Protection and Advanced Threat Protection in the manner
2 described by Finjan.

3 83. Sophos actively updates websites, including Sophos' Support, to promote the Sophos
4 Live Protection and Advanced Threat Protection, including the Sophos Unified Threat Management,
5 Next Generation Firewall, Secure Web Gateway, Secure E-mail Gateway, Sophos Cloud, Endpoint
6 Antivirus Cloud, Endpoint Antivirus, Enduser Protection Suites, and Server Security, to encourage
7 users and developers to practice the methods taught in the '918 Patent.
8

9 **COUNT VI**
10 **(Direct Infringement of the '289 Patent pursuant to 35 U.S.C. § 271(a))**

11 84. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the
12 allegations of the preceding paragraphs, as set forth above.

13 85. Defendant has infringed and continues to infringe one or more claims of the '289
14 Patent in violation of 35 U.S.C. § 271(a).

15 86. Defendant's infringement is based upon literal infringement or, in the alternative,
16 infringement under the doctrine of equivalents.

17 87. Defendant's acts of making, using, importing, selling, and/or offering for sale infringing
18 products and services have been without the permission, consent, authorization or license of Finjan.
19

20 88. Defendant's infringement includes, but is not limited to, the manufacture, use, sale,
21 importation and/or offer for sale of Defendant's products and services, including but not limited to
22 Sophos WebLENS and Sophos Advanced Threat Protection, which embody the patented invention of
23 the '289 Patent.

24 89. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to
25 suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled
26 to preliminary and/or permanent injunctive relief.
27
28

COUNT VII
(Indirect Infringement of the '289 Patent pursuant to 35 U.S.C. § 271(b))

92. Defendant has induced and continues to induce infringement of at least claims 1-9, 19-29, and 35-40 of the '289 Patent under 35 U.S.C. § 271(b).

94. Defendant knowingly and actively aided and abetted the direct infringement of the patent by instructing and encouraging its customers, users and developers to use Sophos WebLENS and Sophos Advanced Threat Protection. Such instructions and encouragement include, but are not limited to, advising third parties to use the Sophos WebLENS and Sophos Advanced Threat Protection in an infringing manner, providing a mechanism through which third parties may use the '289 Patent, specifically through the use of the Sophos WebLENS and Sophos Advanced Threat Protection, advertising and promoting the use of the Sophos WebLENS and Sophos Advanced Threat Protection in an infringing manner, and distributing guidelines and instructions to third parties

1 on how to use the Sophos WebLENS and Sophos Advanced Threat Protection in an infringing
2 manner.

3 95. Sophos regularly updates and maintains the Sophos Support/Labs to provide
4 demonstration, instructions, and technical assistance to users to help them use the Advanced Threat
5 Protection, including:

- 6 • Describing what Advanced Threat Protection is used for and how to adjust its settings. *See*
7 [http://blogs.sophos.com/2014/02/26/whats-coming-in-sophos-utm-accelerated-9-2-5-advanced-](http://blogs.sophos.com/2014/02/26/whats-coming-in-sophos-utm-accelerated-9-2-5-advanced-threat-protection-atp/)
8 [threat-protection-atp/](http://blogs.sophos.com/2014/02/26/whats-coming-in-sophos-utm-accelerated-9-2-5-advanced-threat-protection-atp/), a true and correct copy of which is attached hereto as Exhibit H;
- 9 • Providing a YouTube video on the new feature of Advanced Threat Protection. *Available at*
10 <http://www.youtube.com/watch?v=qcGV-R1z6io> (last visited March 13, 2014);
- 11 • Providing a written “how to” configure the Advanced Threat Protection. *See*
12 <http://www.sophos.com/en-us/support/knowledgebase/120330.aspx>, a true and correct copy of
13 which is attached hereto as Exhibit U.

14 96. Sophos Provides quick start guides, administration guides, user guides, and operating
15 instructions which cover in depth aspects of operating Sophos offerings. *See*
16 <https://www.sophos.com/en-us/support/documentation.aspx>, a true and correct copy of which is
17 attached hereto as Exhibit M.

18 97. Sophos maintains and updates a YouTube channel where training and informational
19 videos are posted in order to promote the use of Sophos products. *See*
20 <http://www.youtube.com/user/SophosGlobalSupport?feature=watch>, a true and correct copy of which
21 is attached hereto as Exhibit N.

22 98. Sophos maintains and promotes the Sophos Partner Program to encourage and expand
23 use of the Sophos Live Protection by offering up-to-date training and certification enabled by a full
24 curriculum of courses in order to increase skills and competency. *See* [http://www.sophos.com/en-](http://www.sophos.com/en-us/partners.aspx)
25 [us/partners.aspx](http://www.sophos.com/en-us/partners.aspx), a true and correct copy of which is attached hereto as Exhibit O; *see also*
26
27
28

1 <http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos-partnership-with-sophos-na.pdf>, a
2 true and correct copy of which is attached hereto as Exhibit P.

3 99. Sophos maintains and promotes the Sophos Managed Service Provider program in
4 which Sophos trains IT personnel to support Sophos products. See [http://www.sophos.com/en-](http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf)
5 [us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf](http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf), a true and correct copy of
6 which is attached hereto as Exhibit Q.

7 100. Sophos provides Global System Integrators who provide advisory, solution and deliver
8 services to its customers across all market sections. These services include consulting, systems
9 integration, managed services and full facilities outsourcing. See [http://www.sophos.com/en-](http://www.sophos.com/en-us/partners/global-system-integrators.aspx)
10 [us/partners/global-system-integrators.aspx](http://www.sophos.com/en-us/partners/global-system-integrators.aspx), a true and correct copy of which is attached hereto as
11 Exhibit R.

12 101. Sophos maintains and offers Sophos Professional Services. Sophos Professional
13 Services plans the requirements of a client security needs, builds the endpoint and network solutions
14 for the clients, and then manages the Sophos implemented solutions. See [http://www.sophos.com/en-](http://www.sophos.com/en-us/medialibrary/PDFs/professionalservices/sophosprofessionalservicesbrna.pdf)
15 [us/medialibrary/PDFs/professionalservices/sophosprofessionalservicesbrna.pdf](http://www.sophos.com/en-us/medialibrary/PDFs/professionalservices/sophosprofessionalservicesbrna.pdf), a true and correct
16 copy of which is attached hereto as Exhibit S.

17 102. Defendant has had knowledge of the '289 Patent at least as of the time it learned of
18 this action for infringement and by continuing the actions described above has had the specific intent
19 to or was willfully blind to the fact that its actions would induce infringement of the '289 Patent.

20 103. Sophos actively and intentionally maintains websites, including Sophos' Support, to
21 promote the Sophos WebLENS and Sophos Advanced Threat Protection and to encourage potential
22 users and developers to use the Sophos WebLENS and Sophos Advanced Threat Protection in the
23 manner described by Finjan.
24
25
26
27
28

1 104. Sophos actively updates websites, including Sophos' Support, to promote the Sophos
2 WebLENS and Sophos Advanced Threat Protection, including the Sophos Unified Threat
3 Management, Virtual Web Appliance Next Generation Firewall, Secure Web Gateway, and Enduser
4 Protection Suites, to encourage users and developers to practice the methods taught in the '289
5 Patent.

6
7 **COUNT VIII**
8 **(Direct Infringement of the '926 Patent pursuant to 35 U.S.C. § 271(a))**

9 105. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the
10 allegations of the preceding paragraphs, as set forth above.

11 106. Defendant has infringed and continues to infringe one or more claims of the '926
12 Patent in violation of 35 U.S.C. § 271(a).

13 107. Defendant's infringement is based upon literal infringement or, in the alternative,
14 infringement under the doctrine of equivalents.

15 108. Defendant's acts of making, using, importing, selling, and/or offering for sale infringing
16 products and services have been without the permission, consent, authorization or license of Finjan.

17 109. Defendant's infringement includes, but is not limited to, the manufacture, use, sale,
18 importation and/or offer for sale of Defendant's products and services, including but not limited to
19 Sophos Live Protection, which embodies the patented invention of the '926 Patent.
20

21 110. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to
22 suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled
23 to preliminary and/or permanent injunctive relief.

24 111. Defendant's infringement of the '926 Patent has injured and continues to injure Finjan
25 in an amount to be proven at trial.
26
27
28

COUNT IX

(Indirect Infringement of the '926 Patent pursuant to 35 U.S.C. § 271(b))

112. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

113. Defendant has induced and continues to induce infringement of at least claims 1-7 and 15-21 of the '926 Patent under 35 U.S.C. § 271(b).

114. In addition to directly infringing the '926 Patent, Defendant indirectly infringes the '926 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including but not limited to its customers, users and developers, to perform some of the steps of the method claims, either literally or under the doctrine of equivalents, of the '926 Patent, where all the steps of the method claims are performed by either Sophos or its customers, users or developers, or some combination thereof. Defendant knew or was willfully blind to the fact that it was inducing others, including customers, users and developers, to infringe by practicing, either themselves or in conjunction with Defendant, one or more method claims of the '926 Patent.

115. Defendant knowingly and actively aided and abetted the direct infringement of the '926 Patent by instructing and encouraging its customers, users and developers to use the Sophos Live Protection. Such instructions and encouragement include but are not limited to, advising third parties to use the Sophos Live Protection in an infringing manner, providing a mechanism through which third parties may infringe the '926 Patent, specifically through the use of the Sophos Live Protection, advertising and promoting the use of the Sophos Live Protection in an infringing manner, and distributing guidelines and instructions to third parties on how to use the Sophos Live Protection in an infringing manner.

1 116. Sophos regularly updates and maintains the Sophos Support/Labs to provide
2 demonstration, instructions, and technical assistance to users to help them use the Sophos Live
3 Protection, including:

- 4 • Providing an overview of how Live Protections works. *See* [http://www.sophos.com/en-](http://www.sophos.com/en-us/support/knowledgebase/111334.aspx)
5 [us/support/knowledgebase/111334.aspx](http://www.sophos.com/en-us/support/knowledgebase/111334.aspx), a true and correct copy of which is attached hereto as
6 Exhibit I;
- 7 • Giving step-by-step instructions on how to turn Live Protection on and off, combined with a
8 video demonstration of the functionalities of Live Protection. *See* [http://www.sophos.com/en-](http://www.sophos.com/en-us/support/knowledgebase/116371.aspx)
9 [us/support/knowledgebase/116371.aspx](http://www.sophos.com/en-us/support/knowledgebase/116371.aspx), a true and correct copy of which is attached hereto as
10 Exhibit J;
- 11 • Maintaining a list of behavior profiles such as SUS/ZelXor-A, created by Sophos' labs and
12 posted on Sophos' website for download. *See* [http://www.sophos.com/en-us/threat-](http://www.sophos.com/en-us/threat-center/threat-analyses/suspicious-behavior-and-files/Sus-ZelXor-A.aspx)
13 [center/threat-analyses/suspicious-behavior-and-files/Sus-ZelXor-A.aspx](http://www.sophos.com/en-us/threat-center/threat-analyses/suspicious-behavior-and-files/Sus-ZelXor-A.aspx), a true and correct
14 copy of which is attached hereto as Exhibit V;
- 15 • Maintaining a list of Live Protection errors and suggesting ways of resolving them. *See*
16 <http://www.sophos.com/en-us/support/knowledgebase/111244.aspx>, a true and correct copy of
17 which is attached hereto as Exhibit L.

18 117. Sophos Provides quick start guides, administration guides, user guides, and operating
19 instructions which cover in depth aspects of operating Sophos offerings. *See*
20 <https://www.sophos.com/en-us/support/documentation.aspx>, a true and correct copy of which is
21 attached hereto as Exhibit M.

22 118. Sophos maintains and updates a YouTube channel where training and informational
23 videos are posted in order to promote the use of Sophos products. *See*
24 <http://www.youtube.com/user/SophosGlobalSupport?feature=watch>, a true and correct copy of which
25 is attached hereto as Exhibit N.

26 119. Sophos maintains and promotes the Sophos Partner Program to encourage and expand
27 use of the Sophos Live Protection by offering up-to-date training and certification enabled by a full
28 curriculum of courses in order to increase skills and competency. *See* [http://www.sophos.com/en-](http://www.sophos.com/en-us/partners.aspx)
[us/partners.aspx](http://www.sophos.com/en-us/partners.aspx), a true and correct copy of which is attached hereto as Exhibit O; *see also*

1 <http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos-partnership-with-sophos-na.pdf>, a
2 true and correct copy of which is attached hereto as Exhibit P.

3 120. Sophos maintains and promotes the Sophos Managed Service Provider program in
4 which Sophos trains IT personnel to support Sophos products. See [http://www.sophos.com/en-](http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf)
5 [us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf](http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf), a true and correct copy of
6 which is attached hereto as Exhibit Q.

7 121. Sophos provides Global System Integrators who provide advisory, solution and deliver
8 services to its customers across all market sections. These services include consulting, systems
9 integration, managed services and full facilities outsourcing. See [http://www.sophos.com/en-](http://www.sophos.com/en-us/partners/global-system-integrators.aspx)
10 [us/partners/global-system-integrators.aspx](http://www.sophos.com/en-us/partners/global-system-integrators.aspx), a true and correct copy of which is attached hereto as
11 Exhibit R.

12 122. Sophos maintains and offers Sophos Professional Services. Sophos Professional
13 Services plans the requirements of a client security needs, builds the endpoint and network solutions
14 for the clients, and then manages the Sophos implemented solutions. See [http://www.sophos.com/en-](http://www.sophos.com/en-us/medialibrary/PDFs/professionalservices/sophosprofessionalservicesbrna.pdf)
15 [us/medialibrary/PDFs/professionalservices/sophosprofessionalservicesbrna.pdf](http://www.sophos.com/en-us/medialibrary/PDFs/professionalservices/sophosprofessionalservicesbrna.pdf), a true and correct
16 copy of which is attached hereto as Exhibit S.

17 123. Defendant has had knowledge of the '926 Patent at least as of the time it learned of
18 this action for infringement and by continuing the actions described above has had the specific intent
19 to or was willfully blind to the fact that its actions would induce infringement of the '926 Patent.

20 124. Sophos actively and intentionally maintains websites, including Sophos' Support, to
21 promote the Sophos Live Protection and to encourage potential users and developers to use the
22 Sophos Live Protection in the manner described by Finjan.
23
24
25
26
27
28

1 125. Sophos actively updates websites, including Sophos' Support, to promote the Sophos
2 Live Protection, including the Sophos Unified Threat Management, Next Generation Firewall, Secure
3 Web Gateway, Secure E-mail Gateway, Sophos Cloud, Endpoint Antivirus Cloud, Endpoint
4 Antivirus, Enduser Protection Suites, and Server Security, to encourage users and developers to
5 practice the methods taught in the '926 Patent.

6
7 **COUNT X**

8 **(Direct Infringement of the '844 Patent pursuant to 35 U.S.C. § 271(a))**

9 126. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the
10 allegations of the preceding paragraphs, as set forth above.

11 127. Defendant has infringed and continues to infringe one or more claims of the '844
12 Patent in violation of 35 U.S.C. § 271(a).

13 128. Defendant's infringement is based upon literal infringement or, in the alternative,
14 infringement under the doctrine of equivalents.

15 129. Defendant's acts of making, using, importing, selling, and/or offering for sale
16 infringing products and services have been without the permission, consent, authorization or license
17 of Finjan.

18 130. Defendant's infringement includes, but is not limited to, the manufacture, use, sale,
19 importation and/or offer for sale of Defendant's products and services, including but not limited to
20 the Sophos Live Protection and Advanced Threat Protection, which embody the patented invention of
21 the '844 Patent.

22 131. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to
23 suffer irreparable harm for which there is no adequate remedy at law. Accordingly, Finjan is entitled
24 to preliminary and/or permanent injunctive relief.
25
26
27
28

1 132. Defendant's infringement of the '844 Patent has injured and continues to injure Finjan
2 in an amount to be proven at trial.

3 **COUNT XI**
4 **(Indirect Infringement of the '844 Patent pursuant to 35 U.S.C. § 271(b))**

5 133. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the
6 allegations of the preceding paragraphs, as set forth above.

7 134. Defendant has induced and continues to induce infringement of at least claims 1-14
8 and 22-31 of the '844 Patent under 35 U.S.C. § 271(b).

9 135. In addition to directly infringing the '844 Patent, Defendant indirectly infringes the
10 '844 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including
11 but not limited to its users and developers, to perform some of the steps of the method claims, either
12 literally or under the doctrine of equivalents, of the '844 Patent, where all the steps of the method
13 claims are performed by either Sophos or its customers, users or developers, or some combination
14 thereof. Defendant knew or was willfully blind to the fact that it was inducing others, including
15 customers, users and developers, to infringe by practicing, either themselves or in conjunction with
16 Defendant, one or more method claims of the '844 Patent.
17

18 136. Defendant knowingly and actively aided and abetted the direct infringement of the
19 '844 Patent by instructing and encouraging its users and developers to use the Sophos Live Protection
20 and Advanced Threat Protection. Such instructions and encouragement include but are not limited to,
21 advising third parties to use the Sophos Live Protection and Advanced Threat Protection in an
22 infringing manner, providing a mechanism through which third parties may infringe the '844 Patent,
23 specifically through the use of the Sophos Live Protection and Advanced Threat Protection,
24 advertising and promoting the use of the Sophos Live Protection and Advanced Threat Protection in
25
26
27
28

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Finjan, Inc. ("Finjan") files this First Amended Complaint for Patent Infringement and Jury Demand against Defendant Sophos, Inc. ("Defendant" or "Sophos") and alleges as follows:

THE PARTIES

1. Finjan is a Delaware corporation, with its corporate headquarters at 1313 N. Market Street, Suite 5100, Wilmington, Delaware 19801. Finjan's U.S. operating business was previously headquartered at 2025 Gateway Place, San Jose, California 95110.

2. Sophos is a Massachusetts corporation with its principal place of business in the United States at 3 Van de Graaff Drive, Second Floor, Burlington, Massachusetts 01803.

JURISDICTION AND VENUE

3. This action arises under the Patent Act, 35 U.S.C. § 101 *et seq.* This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. §§ 1331 and 1338.

4. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b) and (c) and/or 1400(b).

5. This Court has personal jurisdiction over Defendant. Upon information and belief, Defendant does business in this District and has, and continues to, infringe and/or induce the infringement in this District. Sophos operates and maintains an office in this District located at 3945 Freedom Circle, Suite 1100, Santa Clara, California 95054. Currently, Sophos is availing itself of the jurisdiction of Northern California in the *Fortinet, Inc. v. Sophos, Inc.*, 5:13-cv-05831, case. In addition, the Court has personal jurisdiction over Defendant because it has established minimum contacts with the forum and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

1 an infringing manner, and distributing guidelines and instructions to third parties on how to use the
2 Sophos Live Protection and Advanced Threat Protection in an infringing manner.

3 137. Sophos regularly updates and maintains the Sophos Support/Labs to provide
4 demonstration, instructions, and technical assistance to users to help them use the Sophos Live
5 Protection and Advanced Threat Protection, including:

- 6 • Providing an overview of how Live Protections works. See <http://www.sophos.com/en-us/support/knowledgebase/111334.aspx>, a true and correct copy of which is attached hereto as Exhibit I;
- 7 • Giving step-by-step instructions on how to turn Live Protection on and off, combined with a video demonstration of the functionalities of Live Protection. See <http://www.sophos.com/en-us/support/knowledgebase/116371.aspx>, a true and correct copy of which is attached hereto as Exhibit J;
- 8 • Maintaining a list of behavior profiles such as SUS/ZelXor-A, created by Sophos' labs and posted on Sophos' website for download. See <http://www.sophos.com/en-us/threat-center/threat-analyses/suspicious-behavior-and-files/Sus~ZelXor-A.aspx>, a true and correct copy of which is attached hereto as Exhibit W;
- 9 • Maintaining a list of Live Protection errors and suggesting ways of resolving them. See <http://www.sophos.com/en-us/support/knowledgebase/111244.aspx>, a true and correct copy of which is attached hereto as Exhibit L;
- 10 • Describing what Advanced Threat Protection is used for and how to adjust its settings. See <http://blogs.sophos.com/2014/02/26/whats-coming-in-sophos-utm-accelerated-9-2-5-advanced-threat-protection-atp/>, a true and correct copy of which is attached hereto as Exhibit H;
- 11 • Providing a YouTube video on the new feature of Advanced Threat Protection. Available at <http://www.youtube.com/watch?v=qcGV-R1z6io> (last visited March 13, 2014);
- 12 • Providing a written "how to" configure the Advanced Threat Protection. See <http://www.sophos.com/en-us/support/knowledgebase/120330.aspx>, a true and correct copy of which is attached hereto as Exhibit U.

13 138. Sophos Provides quick start guides, administration guides, user guides, and operating
14 instructions which cover in depth aspects of operating Sophos offerings. See
15 <https://www.sophos.com/en-us/support/documentation.aspx>, a true and correct copy of which is
16 attached hereto as Exhibit M.

1 139. Sophos maintains and updates a YouTube channel where training and informational
2 videos are posted in order to promote the use of Sophos products. *See*
3 <http://www.youtube.com/user/SophosGlobalSupport?feature=watch>, a true and correct copy of which
4 is attached hereto as Exhibit N.

5 140. Sophos maintains and promotes the Sophos Partner Program to encourage and expand
6 use of the Sophos Live Protection by offering up-to-date training and certification enabled by a full
7 curriculum of courses in order to increase skills and competency. *See* [http://www.sophos.com/en-](http://www.sophos.com/en-us/partners.aspx)
8 [us/partners.aspx](http://www.sophos.com/en-us/partners.aspx), a true and correct copy of which is attached hereto as Exhibit O; *see also*
9 <http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos-partnership-with-sophos-na.pdf>, a
10 true and correct copy of which is attached hereto as Exhibit P.

11 141. Sophos maintains and promotes the Sophos Managed Service Provider program in
12 which Sophos trains IT personnel to support Sophos products. *See* [http://www.sophos.com/en-](http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf)
13 [us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf](http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophos_complete_security_msps_dsna.pdf), a true and correct copy of
14 which is attached hereto as Exhibit Q.

15 142. Sophos provides Global System Integrators who provide advisory, solution and deliver
16 services to its customers across all market sections. These services include consulting, systems
17 integration, managed services and full facilities outsourcing. *See* [http://www.sophos.com/en-](http://www.sophos.com/en-us/partners/global-system-integrators.aspx)
18 [us/partners/global-system-integrators.aspx](http://www.sophos.com/en-us/partners/global-system-integrators.aspx), a true and correct copy of which is attached hereto as
19 Exhibit R.

20 143. Sophos maintains and offers Sophos Professional Services. Sophos Professional
21 Services plans the requirements of a client security needs, builds the endpoint and network solutions
22 for the clients, and then manages the Sophos implemented solutions. *See* <http://www.sophos.com/en->
23 [us/](http://www.sophos.com/en-)

1 [us/medialibrary/PDFs/professionalservices/sophosprofessionalservicesbrna.pdf](http://us.medialibrary/PDFs/professionalservices/sophosprofessionalservicesbrna.pdf), a true and correct
2 copy of which is attached hereto as Exhibit S.

3 144. Defendant has had knowledge of the '844 Patent at least as of the time it learned of
4 this action for infringement and by continuing the actions described above has had the specific intent
5 to or was willfully blind to the fact that its actions would induce infringement of the '844 Patent.

6 145. Sophos actively and intentionally maintains websites, including Sophos' Support, to
7 promote the Sophos Live Protection and Advanced Threat Protection and to encourage potential users
8 and developers to use the Sophos Live Protection and Advanced Threat Protection in the manner
9 described by Finjan.
10

11 146. Sophos actively updates websites, including Sophos' Support, to promote the Sophos
12 Live Protection and Advanced Threat Protection, including the Sophos Unified Threat Management,
13 Next Generation Firewall, Secure Web Gateway, Secure E-mail Gateway, Sophos Cloud, Endpoint
14 Antivirus Cloud, Endpoint Antivirus, Enduser Protection Suites, and Server Security, to encourage
15 users and developers to practice the methods taught in the '844 Patent.
16

17 **PRAYER FOR RELIEF**

18 WHEREFORE, Finjan prays for judgment and relief as follows:

19 A. An entry of judgment holding Defendant has infringed and is infringing the '780
20 Patent, the '154 Patent, the '918 Patent, the '289 Patent, the '926 Patent, and the '844 Patent; and
21 Defendant has induced and is inducing infringement of the '780 Patent, the '918 Patent, the '289
22 Patent, the '926 Patent, and the '844 Patent;
23

24 B. A preliminary and permanent injunction against Defendant and its officers, employees,
25 agents, servants, attorneys, instrumentalities, and/or those in privity with them, from infringing, or
26 inducing the infringement of the '780 Patent, the '154 Patent, the '918 Patent, the '289 Patent, the
27
28

1 926 Patent, and the '844 Patent, and for all further and proper injunctive relief pursuant to 35 U.S.C.
2 § 283;

3 C. An award to Finjan of such damages as it shall prove at trial against Defendant that is
4 adequate to fully compensate Finjan for Defendant's infringement the '780 Patent, the '154 Patent,
5 the '918 Patent, the '289 Patent, the 926 Patent, and the '844 Patent, said damages to be no less than a
6 reasonable royalty;

7
8 D. A finding that this case is "exceptional" and an award to Finjan of its costs and
9 reasonable attorney's fees, as provided by 35 U.S.C. § 285;

10 E. An accounting of all infringing sales and revenues, together with post judgment
11 interest and prejudgment interest from the first date of infringement of the '780 Patent, the '154
12 Patent, the '918 Patent, the '289 Patent, the '926 Patent, and the '844 Patent; and

13 F. Such further and other relief as the Court may deem proper and just.
14

15 Respectfully submitted,

16 Dated: March 14, 2014

By: /s/ Paul J. Andre

17 Paul J. Andre
18 Lisa Kobiaalka
19 James Hannah
20 KRAMER LEVIN NAFTALIS
& FRANKEL LLP
21 990 Marsh Road
Menlo Park, CA 94025
22 Telephone: (650) 752-1700
Facsimile: (650) 752-1800
23 pandre@kramerlevin.com
lkobiaalka@kramerlevin.com
jhannah@kramerlevin.com

24 *Attorneys for Plaintiff*
25 FINJAN, INC.
26
27
28

DEMAND FOR JURY TRIAL

Finjan demands a jury trial on all issues so triable.

Respectfully submitted,

Dated: March 14, 2014

By: /s/ Paul J. Andre

Paul J. Andre

Lisa Kobialka

James Hannah

KRAMER LEVIN NAFTALIS

& FRANKEL LLP

990 Marsh Road

Menlo Park, CA 94025

Telephone: (650) 752-1700

Facsimile: (650) 752-1800

pandre@kramerlevin.com

lkobialka@kramerlevin.com

jhannah@kramerlevin.com

Attorneys for Plaintiff

FINJAN, INC.

INTRADISTRICT ASSIGNMENT

6. Pursuant to Local Rule 3-2(c), Intellectual Property actions are assigned on a district-wide basis.

FINJAN'S INNOVATIONS

7. Finjan was founded in 1997 as a wholly-owned subsidiary of Finjan Software Ltd., an Israeli corporation. Finjan was a pioneer in developing proactive security technologies capable of detecting previously unknown and emerging online security threats recognized today under the umbrella of "malware." These technologies protect networks and endpoints by identifying suspicious patterns and behaviors of content delivered over the Internet. Finjan has been awarded, and continues to prosecute, numerous patents in the United States and around the world resulting directly from Finjan's more than decade-long research and development efforts, supported by a dozen inventors.

8. Finjan built and sold software, including APIs, and appliances for network security using these patented technologies. These products and customers continue to be supported by Finjan's licensing partners. At its height, Finjan employed nearly 150 employees around the world building and selling security products and operating the Malicious Code Research Center through which it frequently published research regarding network security and current threats on the Internet. Finjan's pioneering approach to online security drew equity investments from two major software and technology companies, the first in 2005, followed by the second in 2006. Through 2009, Finjan has generated millions of dollars in product sales and related services and support revenues.

9. Finjan's founder and original investors are still involved with and invested in the company today, as are a number of other key executives and advisors. Currently, Finjan is a technology company applying its research, development, knowledge and experience with security technologies to working with inventors, investing in and/or acquiring other technology companies,

1 investing in a variety of research organizations, and evaluating strategic partnerships with large
2 companies.

3 10. On October 12, 2004, U.S. Patent No. 6,804,780 ("the '780 Patent"), entitled
4 SYSTEM AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM
5 HOSTILE DOWNLOADABLES, was issued to Shlomo Touboul. A true and correct copy of the
6 '780 Patent is attached to this Complaint as Exhibit A and is incorporated by reference herein.

7
8 11. All rights, title, and interest in the '780 Patent have been assigned to Finjan, which is
9 the sole owner of the '780 Patent. Finjan has been the sole owner of the '780 Patent since its
10 issuance.

11 12. The '780 Patent is generally directed towards methods and systems for generating a
12 Downloadable ID. By generating an identification for each examined Downloadable, the system
13 may allow for the Downloadable to be recognized without reevaluation. Such recognition increases
14 efficiency while also saving valuable resources, such as memory and computing power.

15
16 13. On March 20, 2012, U.S. Patent No. 8,141,154 ("the '154 Patent"), entitled SYSTEM
17 AND METHOD FOR INSPECTING DYNAMICALLY GENERATED EXECUTABLE CODE, was
18 issued to David Gruzman and Yuval Ben-Itzhak. A true and correct copy of the '154 Patent is
19 attached to this Complaint as Exhibit B and is incorporated by reference herein.

20 14. All rights, title, and interest in the '154 Patent have been assigned to Finjan, who is the
21 sole owner of the '154 Patent. Finjan has been the sole owner of the '154 Patent since its issuance.

22
23 15. The '154 Patent is generally directed towards a gateway computer for protecting a
24 client computer from dynamically generated malicious content. One way this is accomplished is to
25 use a content processor to process a first function and invoke a second function if a security computer
26 indicates that it is safe to invoke the second function.

1 16. On November 3, 2009, U.S. Patent No. 7,613,918 ("the '918 Patent"), entitled
2 SYSTEM AND METHOD FOR ENFORCING A SECURITY CONTEXT ON A
3 DOWNLOADABLE, was issued to Yuval Ben-Itzhak. A true and correct copy of the '918 Patent is
4 attached to this Complaint as Exhibit C and is incorporated by reference herein.

5 17. All rights, title, and interest in the '918 Patent have been assigned to Finjan, who is the
6 sole owner of the '918 Patent. Finjan has been the sole owner of the '918 Patent since its issuance.

7 18. The '918 Patent is generally directed to a system and method for enforcing a security
8 context on a Downloadable. One way this is accomplished is by making use of security contexts that
9 are associated within certain user/group computer accounts when deriving a profile for code received
10 from the Internet.

11 19. On July 13, 2010, U.S. Patent No. 7,757,289 ("the '289 Patent"), entitled SYSTEM
12 AND METHOD FOR INSPECTING DYNAMICALLY GENERATED EXECUTABLE CODE, was
13 issued to David Gruzman and Yuval Ben-Itzhak. A true and correct copy of the '289 Patent is
14 attached to this Complaint as Exhibit D and is incorporated by reference herein.

15 20. All rights, title, and interest in the '289 Patent have been assigned to Finjan, which is
16 the sole owner of the '289 Patent. Finjan has been the sole owner of the '289 Patent since its
17 issuance.

18 21. The '289 Patent generally covers a system and method for inspecting dynamically
19 generated executable code. The claims generally cover receiving content with an original call
20 function and replacing the original call function with a substitute call function, and then determining
21 whether it is safe to invoke the original call function.

22 22. On November 3, 2009, U.S. Patent No. 7,613,926 ("the '926 Patent"), entitled
23 METHOD AND SYSTEM FOR PROTECTING A COMPUTER AND A NETWORK FROM
24

1 HOSTILE DOWNLOADABLES, was issued to Yigal Mordechai Edery, Nimrod Itzhak Vered,
2 David R. Kroll and Shlomo Touboul. A true and correct copy of the '926 Patent is attached to this
3 Complaint as Exhibit E and is incorporated by reference herein.

4 23. All rights, title, and interest in the '926 Patent have been assigned to Finjan, which is
5 the sole owner of the '926 Patent. Finjan has been the sole owner of the '926 Patent since its
6 issuance.

7 24. The '926 Patent generally covers a method and system for protecting a computer and a
8 network from hostile downloadables. The claims generally cover performing hashing on a
9 downloadable in order to generate a downloadable ID, retrieving security profile data, and
10 transmitting an appended downloadable.
11

12 25. On November 28, 2000, U.S. Patent No. 6,154,844 ("the '844 Patent"), entitled
13 SYSTEM AND METHOD FOR ATTACHING A DOWNLOADABLE SECURITY PROFILE TO
14 A DOWNLOADABLE, was issued to Shlomo Touboul and Nachshon Gal. A true and correct copy
15 of the '844 Patent is attached to this Complaint as Exhibit F and is incorporated by reference herein.
16

17 26. All rights, title, and interest in the '844 Patent have been assigned to Finjan, who is the
18 sole owner of the '844 Patent. Finjan has been the sole owner of the '844 Patent since its issuance.

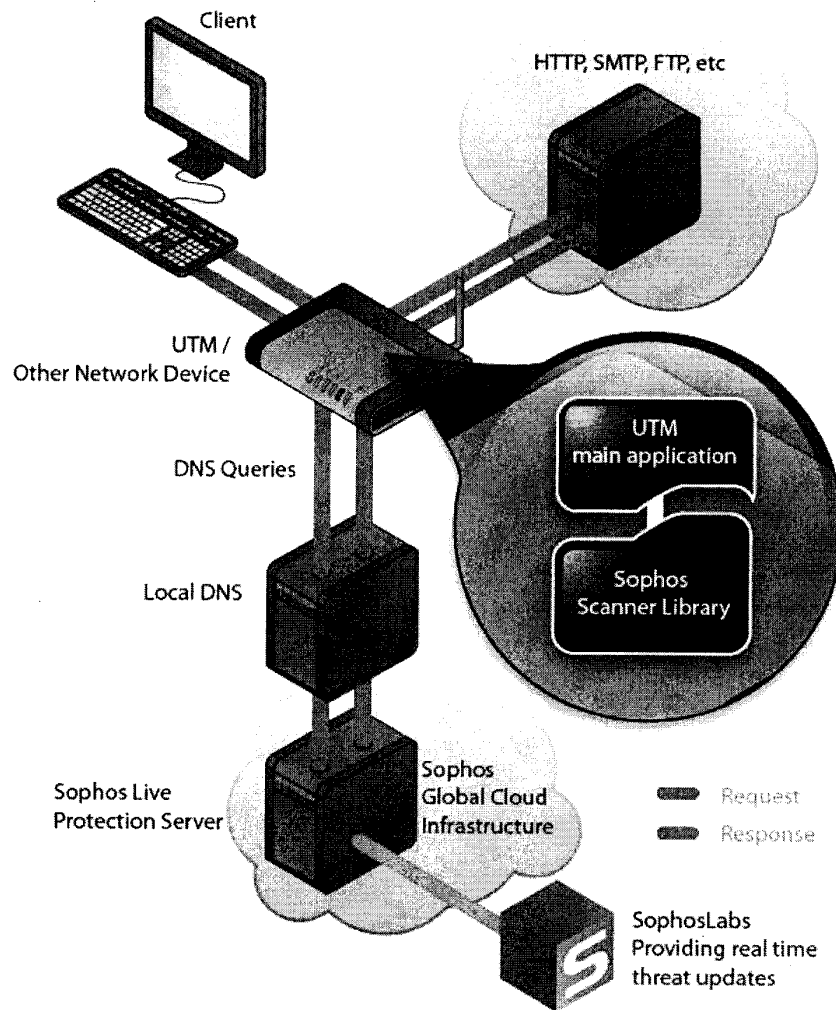
19 27. The '844 Patent is generally directed towards computer networks, and more
20 particularly, provides a system that protects devices connected to the Internet from undesirable
21 operations from web-based content. One of the ways this is accomplished is by linking a security
22 profile to such web-based content to facilitate the protection of computers and networks from
23 malicious web-based content.
24
25
26
27
28

SOPHOS

1
2 28. Sophos makes, uses, sells, offers for sale, and/or imports into the United States and
3 this District products and services that utilize the Sophos Live Protection, Advanced Threat
4 Protection, and WebLENS, including without limitation on Enduser Protection Suites, Endpoint
5 Antivirus, Endpoint Antivirus Cloud, Sophos Cloud, Unified Threat Management, Next-Gen
6 Firewall, Secure Web Gateway, Secure Email Gateway, and Server Security.

7
8 29. Sophos products are broken down into three broad categories. The first category is
9 Network Security products which are used to protect a network of computer and mobile devices both
10 remotely and locally. The Network Security products generally sit at the gateway between a client
11 device and the Internet. These Network Security products can include firewalls, UTMs, Wi-Fi, VPN,
12 web and e-mail protection. The second category is EndUser Protection which generally resides as
13 software on client devices such as personal computers, smart phones, tablets, and laptops. The third
14 category is Server Protection, which generally provides antivirus protection for servers.

15
16 30. Sophos Live Protection is offered with Sophos Network Protection products, EndUser
17 Protection products, and Server Protection products. Live Protection will perform instant lookup of
18 suspicious files in the cloud and compare them to the Sophos Labs database. This happens when a
19 file has been identified as suspicious, but locally the determination cannot be made whether it is a
20 safe. If the file is identified as clean or malicious by Sophos Live Protection, the decision is sent back
21 to the endpoint or network device. Live Protection may also be used for cloud lookups of URIs and
22 automatically and dynamically categorize any URIs that have not been visited by a user. Finally,
23 Live Protection will use live cloud lookups for checksum detections in order to stop malware through
24 email attachments, IM and other protocols. The following diagram depicts generally how Live
25 Protection functions:
26
27
28



See <http://www.sophos.com/en-us/medialibrary/PDFs/partners/sophosliveprotectiondsna.ashx>, a true and correct copy of which is attached hereto as Exhibit G.

31. Recently, Sophos Advanced Threat Protection was introduced and can be found in Sophos Network Protection products. Sophos Advanced Threat Protection is supported with data from the Sophos network of labs and leverages data from the intrusion prevention system and web protection in order to combat Advanced Persistent Threats. Sophos Advanced Threat Protection may

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint:



Practitioners associated with Customer Number:

115222

OR



Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number

Name	Registration Number

As attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignments documents attached to this form in accordance with 37 CFR 3.73(c).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to:



The address associated with Customer Number:

115222

OR


<input type="checkbox"/> Firm or Individual Name			
Address			
City	State	Zip	
Country			
Telephone	Email		

Assignee Name and Address: Finjan, Inc.
c/o Pepper Hamilton LLP
1315 Market Street
Hercules Plaza, Suite 5100
Wilmington, DE 19809-1709

A copy of this form, together with a statement under 37 CFR 3.73(c) (Form PTO/AIA/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(c) may be completed by one of The practitioners appointed in this form, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature		Date	1/13/14
Name	Philip Hartstein	Telephone	646-568-2091
Title	President of Finjan Holdings, Inc., parent to Finjan, Inc.		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

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

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Finjan, Inc.

Application No./Patent No.: 11/370,114 / 7,613,926

Filed/Issue Date: March 7, 2006 / November 3, 1999

Titled: Method and System for Protecting a Computer and a Network From Hostile Downloadables

Finjan, Inc., a corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☒ the assignee of the entire right, title, and interest in;
2. ☐ an assignee of less than the entire right, title, and interest in
(The extent (by percentage) of its ownership interest is _____ %); or
3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

- A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy therefore is attached.

OR

- B. ☒ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Yigal M. Eder, Nimrod I. Vered, David R. Krell To: Finjan Software, Ltd.

The document was recorded in the United States Patent and Trademark Office at
Reel 033753, Frame 0574, or for which a copy thereof is attached.

2. From: Shlomo Touboul To: Finjan Software, Ltd.

The document was recorded in the United States Patent and Trademark Office at
Reel 033753, Frame 0546, or for which a copy thereof is attached.

3. From: Finjan Software, Ltd. To: Finjan, Inc.

The document was recorded in the United States Patent and Trademark Office at
Reel 023556, Frame 0853, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

- ☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Dawn-Marie Bey/

Signature

September 19, 2014

Date

Dawn-Marie Bey

Printed or Typed Name

Partner - 44,442

Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Electronic Acknowledgement Receipt	
EFS ID:	20192259
Application Number:	11370114
International Application Number:	
Confirmation Number:	1442
Title of Invention:	METHOD AND SYSTEM FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE DOWNLOADABLES
First Named Inventor/Applicant Name:	Yigal Mordechai Edery
Customer Number:	115222
Filer:	Dawn-Marie Bey./Jeanne Paoella-Bald
Filer Authorized By:	Dawn-Marie Bey.
Attorney Docket Number:	FIN0001CON1CIP1CON2
Receipt Date:	19-SEP-2014
Filing Date:	07-MAR-2006
Time Stamp:	15:40:35
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	Power of Attorney	finjaninc_executed_generalpo a.pdf	1912351 43623b0f91a796abeeb37a02a7ba8f94281f bea1	no	1

Warnings:

Information:

2	Assignee showing of ownership per 37 CFR 3.73.	7613926_executed_373bstatement.pdf	103036 <small>96d2002d289041413eb51746483857a790215630</small>	no	1
Warnings:					
Information:					
Total Files Size (in bytes):				2015387	
<p>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.</p> <p><u>New Applications Under 35 U.S.C. 111</u> 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.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> 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.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> 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.</p>					



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/370,114	03/07/2006	Yigal Mordechai Edery	FIN0001CON1CIP1CON2

CONFIRMATION NO. 1442

POA ACCEPTANCE LETTER

115222
Bey & Cotropia PLLC (Finjan Inc.)
213 Bayly Court
Richmond, VA 23229



Date Mailed: 09/26/2014

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 09/19/2014.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/sibrahim/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/370,114	03/07/2006	Yigal Mordechai Edery	FIN0001CON1CIP1CON2

CONFIRMATION NO. 1442

POWER OF ATTORNEY NOTICE

115222

Bey & Cotropia PLLC (Finjan Inc.)
213 Bayly Court
Richmond, VA 23229



OC000000070968811

Date Mailed: 09/26/2014

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 09/19/2014.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/s/brahim/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

AO 120 (Rev. 2/99)

TO: Mail Stop 8 Director of the U.S. Patent & Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been
filed in the U.S. District Court Northern District California on the ☒ Patents or ☐ Trademarks:

DOCKET NO. CV 14-02998 RS	DATE FILED June 30, 2014	U.S. DISTRICT COURT 450 Golden Gate Avenue, 16 th Floor, San Francisco CA 94102
PLAINTIFF FINJAN INC		DEFENDANT SYMANTEC CORP
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 6,154,844		
2 7,613,926		
3 7,756,996		
4 7,757,289		
5 7,930,299		

In the above—entitled case, the following patent(s) have been included:

DATE INCLUDED	INCLUDED BY <input checked="" type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8,015,182		***see Attach First Amended Complaint***
2 8,141,154		
3 8,677,494		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK Richard W. Wicking	(BY) DEPUTY CLERK Gina Augustine	DATE September 18, 2014
-----------------------------	-------------------------------------	----------------------------

Copy 1—Upon initiation of action, mail this copy to Commissioner Copy 3—Upon termination of action, mail this copy to Commissioner
Copy 2—Upon filing document adding patent(s), mail this copy to Commissioner Copy 4—Case file copy

TO: Mail Stop 8 Director of the U.S. Patent & Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been
 filed in the U.S. District Court Northern District of California on the following ☒ Patents or ☐ Trademarks:

DOCKET NO. CV 14-04908 JSC	DATE FILED 11/4/2014	U.S. DISTRICT COURT 450 Golden Gate Avenue, P.O. Box 36060, San Francisco, CA 94102
PLAINTIFF FINJAN INC		DEFENDANT PALO ALTO NETWORKS INC
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 see Complaint		
2 6,804,780		
3 6,965,968		
4 7,058,822		
5 7,418,731		

In the above—entitled case, the following patent(s) have been included:

DATE INCLUDED	INCLUDED BY <input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading		
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK	
1 7,613,918			
2 7,613,926			
3 7,647,633			
4 8,141,154			
5 8,225,408			
8,677,494			

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK Richard W. Wicking	(BY) DEPUTY CLERK Sheila Rash	DATE November 5, 2014
-----------------------------	----------------------------------	--------------------------

Copy 1—Upon initiation of action, mail this copy to Commissioner Copy 3—Upon termination of action, mail this copy to Commissioner
 Copy 2—Upon filing document adding patent(s), mail this copy to Commissioner Copy 4—Case file copy