(12) **EX PARTE REEXAMINATION CERTIFICATE** (10815th)

United States Patent
Edery et al.

(10) **Number:** US 7,058,822 C1

(45) **Certificate Issued:** Feb. 16, 2016

(54) **MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS**

(75) Inventors: **Yigal Mordechai Edery**, Pardesia, IL (US); **Nimrod Itzhak Vered**, Goosh Tel-Mond, IL (US); **David R. Kroll**, San Jose, CA (US); **Shlomo Touboul**, Kefar-Haim (IL)

(73) Assignee: **Finjan, Inc.**

Reexamination Request:
No. 90/013,017, Oct. 7, 2013

Reexamination Certificate for:
Patent No.:	**7,058,822**
Issued:	**Jun. 6, 2006**
Appl. No.:	**09/861,229**
Filed:	**May 17, 2001**

Certificate of Correction issued Nov. 27, 2012

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/539,667, filed on Mar. 30, 2000, now Pat. No. 6,804,780, which is a continuation of application No. 08/964,388, filed on Nov. 6, 1997, now Pat. No. 6,092,194, said application No. 09/861,229 is a continuation-in-part of application No. 09/551,302, filed on Apr. 18, 2000, now Pat. No. 6,480,962, which is a continuation of application No. 08/790,097, filed on Jan. 29, 1997, now Pat. No. 6,167,520.

(60) Provisional application No. 60/205,591, filed on May 17, 2000.

(51) **Int. Cl.**
G06F 11/30	(2006.01)
H04L 29/06	(2006.01)
G06F 21/53	(2013.01)
G06F 21/56	(2013.01)
G06F 21/52	(2013.01)

(52) **U.S. Cl.**
CPC *H04L 63/145* (2013.01); *G06F 21/52* (2013.01); *G06F 21/53* (2013.01); *G06F 21/562* (2013.01); *H04L 63/1408* (2013.01); *H04L 63/1441* (2013.01); *H04L 63/20* (2013.01); *G06F 2221/2119* (2013.01); *G06F 2221/2141* (2013.01)

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

(56) **References Cited**

To view the complete listing of prior art documents cited during the proceeding for Reexamination Control Number 90/013,017, please refer to the USPTO's public Patent Application Information Retrieval (PAIR) system under the Display References tab.

Primary Examiner — Adam L Basehoar

(57) **ABSTRACT**

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/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 a 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 in response to the attempts, more suitably in conjunction with protection policies.

1
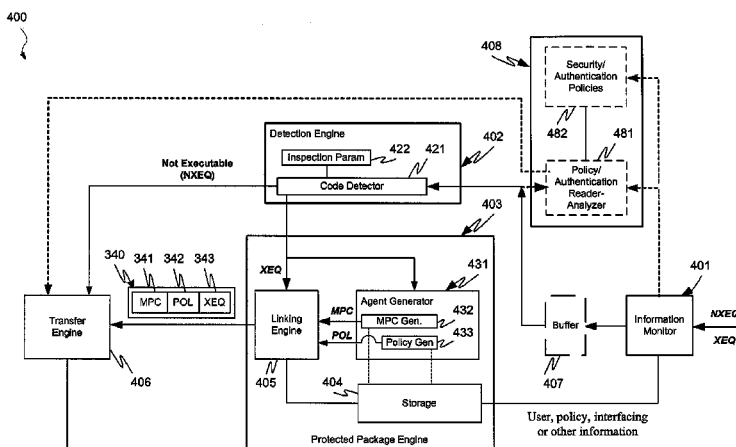
EX PARTE
REEXAMINATION CERTIFICATE

THE PATENT IS HEREBY AMENDED AS
INDICATED BELOW.

**Matter enclosed in heavy brackets [ ] appeared in the
patent, but has been deleted and is no longer a part of the
patent; matter printed in italics indicates additions made
to the patent.**

ONLY THOSE PARAGRAPHS OF THE
SPECIFICATION AFFECTED BY AMENDMENT
ARE PRINTED HEREIN.

Column 1, line 7 to Column 1, line 21:

This application claims benefit and hereby incorporates by
reference provisional application Ser. No. 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 appli-
cation Ser. No. 09/539,667, now U.S. Pat. No. 6,804,780,
entitled "System and Method for Protecting a Computer and
Network From Hostile Downloadables" filed on Mar. 30,
2000 by inventor Shlomo Touboul, *which is a continuation of
U.S. patent application Ser. No. 08/964,388, now U.S. Pat.
No. 6,092,194, entitled "System and Method for Protecting a
Computer and a Network from Hostile Downloadables" filed
on Nov. 6, 1997 by inventor Shlomo Touboul.* This application
is also a Continuation-In-Part of and hereby incorporates by
reference patent application Ser. No. 09/551,302, now U.S.
Pat. No. 6,480,962 entitled "System and Method for Protect-
ing a Client During Runtime From Hostile Downloadables",
filed on Apr. 18, 2000 by inventor Shlomo Touboul, *which is
a continuation of U.S. application Ser. No. 08/790,097, now
U.S. Pat. No. 6,167,520 entitled "System and Method For
Protecting a Client From Hostile Downloadables", filed Jan.
29, 1997 by inventor Shlomo Touboul.*

AS A RESULT OF REEXAMINATION, IT HAS BEEN
DETERMINED THAT:

The patentability of claims **1-8** and **16-27** is confirmed.
New claims **36** and **37** are added and determined to be
patentable.
Claims **9-15** and **28-35** were not reexamined.

2

36. A processor-based system, comprising:

an information monitor for receiving downloadable-infor-
mation;

a content inspection engine communicatively coupled to
the information monitor for determining whether the
downloadable-information includes executable code,
wherein determining whether the downloadable-infor-
mation includes executable code includes analyzing
downloadable-information for operations to be
executed on a computer; and

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

wherein the packaging engine comprises an MPC genera-
tor for providing the MPC, a linking engine coupled to
the MPC generator for forming a sandbox package
including the MPC and the downloadable-information,
and a transfer engine for causing the sandbox package
to be communicated to the at least one information-
destination.

37. A processor-based method, comprising:

receiving by a server downloadable-information;

determining by a content inspection engine associated with
the server whether the downloadable-information
includes executable code, wherein determining whether
the downloadable-information includes executable
code includes analyzing downloadable-information for
one or more operations to be executed on a computer;
and

causing by a transfer engine associated with the server
mobile protection code to be communicated to at least
one information-destination of the downloadable-infor-
mation, if the downloadable-information is determined
to include executable code,

wherein the causing mobile protection code to be commu-
nicated comprises forming by a packaging engine a
sandboxed package including the mobile protection
code and the downloadable-information, and causing
by the transfer engine the sandboxed package to be
communicated to the at least one information-destina-
tion.

* * * * *