

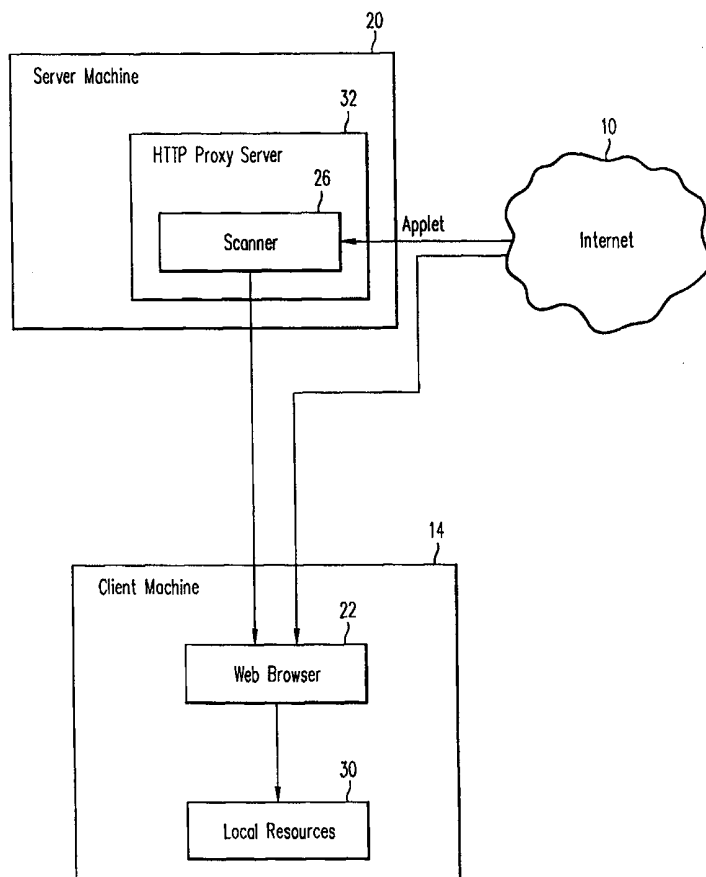


INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : G06F 11/00	A1	(11) International Publication Number: WO 99/13402 (43) International Publication Date: 18 March 1999 (18.03.99)
(21) International Application Number: PCT/US98/15807 (22) International Filing Date: 14 August 1998 (14.08.98) (30) Priority Data: 08/926,619 10 September 1997 (10.09.97) US (71) Applicant: TREND MICRO, INC. [US/US]; 10101 N. De Anza Boulevard, Cupertino, CA 95014 (US). (72) Inventor: JI, Shuang; 98 Muir Avenue, Santa Clara, CA 95051 (US). (74) Agents: KLIVANS, Norman, R. et al.; Skjerven, Morrill, MacPherson, Franklin & Friel LLP, Suite 700, 25 Metro Drive, San Jose, CA 95110 (US).		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i> <i>With amended claims.</i>

(54) Title: COMPUTER NETWORK MALICIOUS CODE SCANNER**(57) Abstract**

A network scanner (26) for security checking of application programs (e.g. Java applets or Active X controls) received over the Internet or an Intranet (10) has both static (pre-run time) and dynamic (run time) scanning. Static scanning at the HTTP proxy server (32) identifies suspicious instructions and instruments them e.g. a pre-and post-filter instruction sequence or otherwise. The instrumented applet is then transferred to the client (14) (web browser (22)) together with security monitoring code. During run time at the client (14), the instrumented instructions are thereby monitored for security policy violations, and execution of an instruction is prevented in the event of such a violation.



FOR THE PURPOSES OF INFORMATION ONLY

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

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

COMPUTER NETWORK MALICIOUS CODE SCANNER

5 FIELD OF THE INVENTION

 This invention pertains to computer networks and specifically to detecting and preventing operation of computer viruses and other types of malicious computer code.

10

BACKGROUND

 With the rapid development of the Internet, Intranet, and network computing, applications (application programs) are distributed more and more
15 via such networks, instead of via physical storage media. Many associated distribution technologies are available, such as Java and Active X. Therefore objects with both data and code flow around the network and have seamless integration with local computer
20 resources. However, this also poses a great security risk to users. Code (software) from unknown origin is thereby executed on local computers and given access to local resources such as the hard disk drive in a user's computer. In a world wide web browser environment,
25 such code is often automatically executed and the user might not even have a chance to be forewarned about any security risks (e.g. presence of computer viruses) he bears. Attempts have been made to reduce such risks; see Ji et al., U.S. Patent 5,623,600, incorporated by
30 reference in its entirety.

Active X technology, like Java, distributes code that can access local system resources directly. The web browser cannot monitor or block such accesses. Such an applet (application) can do virtually anything that a conventional program, for instance, a virus, is capable of doing. Microsoft Corp. and others have attempted to address this problem by using digital signature technology, whereby a special algorithm generates a digital profile of the applet. The profile is attached to the applet. When an applet is downloaded from the Internet, a verification algorithm is run on the applet and the digital profile to ensure that the applet code has not been modified after the signing. If an applet is signed by a known signature, it is considered safe.

However, no analysis of the code is done to check the behavior of the applet. It is not difficult to obtain a signature from a reputable source, since the signature can be applied for online. It has occurred that a person has created an Active X applet that was authenticated by Microsoft but contains malicious code. (Malicious code refers to viruses and other problematic software. A virus is a program intended to replicate and damage operation of a computer system without the user's knowledge or permission. In the Internet/Java environment, the replication aspect may not be present, hence the term "malicious code" broadly referring to such damaging software even if it does not replicate.)

Java being an interpreted language, Java code can be monitored at run-time. Most web browsers block

attempts to access local resources by Java applets,
which protects the local computer to a certain extent.
However, as the popularity of Intranets (private
Internets) increases, more and more applets need to
5 have access to local computers. Such restrictions
posed by the web browsers are becoming rather
inconvenient. As a result, web browsers are relaxing
their security policies. Netscape Communicator is a
web browser that now gives users the ability to
10 selectively run applets with known security risks.
Again, decisions are made based on trust, with no code
analysis done.

Hence scanning programs with the ability to
analyze and monitor applets are in need to protect
15 users.

At least three Java applet scanners are currently
available commercially: SurfinShield and SurfinGate,
both from Finjan, and Cage from Digitivity, Inc.
SurfinShield is a client-side (user) solution. A copy
20 of SurfinShield must be installed on every computer
which is running a web browser. SurfinShield replaces
some of the Java library functions included in the
browser that may pose security risks with its own.
This way, it can trap all such calls and block them if
25 necessary.

SurfinShield provides run-time monitoring. It
introduces almost no performance overhead on applet
startup and execution. It is able to trap all security
breach attempts, if a correct set of Java library
30 functions is replaced. However, it is still difficult

to keep track of the states of individual applets if a series of actions must be performed by the instances before they can be determined dangerous this way, because the scanner is activated rather passively by
5 the applets.

Since every computer in an organization needs a copy of the SurfinShield software, it is expensive to deploy. Also, installing a new release of the product involves updating on every computer, imposing a
10 significant administrative burden.

Because SurfinShield replaces library functions of browsers, it is also browser-dependent; a minor browser upgrade may prevent operation. SufinGate is a server solution that is installed on an HTTP proxy server.
15 Therefore, one copy of the software can protect all the computers proxied by that server. Unlike SufinShield, SurfinGate only scans the applet code statically. If it detects that one or more insecure functions might be called during the execution of the applet, it blocks
20 the applet. Its scanning algorithm is rather slow. To solve this problem, SurfinGate maintains an applet profile database. Each applet is given an ID which is its URL. Once an applet is scanned, an entry is added to the database with its applet ID and the insecure
25 functions it might try to access. When this applet is downloaded again, the security profile is taken from the database to determine the behavior of the applet. No analysis is redone. This means that if a previously safe applet is modified and still has the same URL,
30 SurfinGate will fail to rescan it and let it pass

through. Also, because the size of the database is ever-growing, its maintenance becomes a problem over time.

Cage is also a server solution that is installed on an HTTP proxy server, and provides run-time monitoring and yet avoids client-side installations or changes. It is similar to X Windows. All workstations protected by the server serve as X terminals and only provide graphical presentation functionality. When an applet is downloaded to Cage, it stops at the Cage server and only a GUI (graphical user interface) agent in the form of an applet is passed back to the browser. The applet is then run on the Cage server. GUI requests are passed to the agent on the client, which draws the presentation for the user. Therefore, it appears to users that the applets are actually running locally.

This approach creates a heavy load on the server, since all the applets in the protected domain run on the server and all the potentially powerful computers are used as graphical terminals only. Also, reasonable requests to access local resources (as in Intranet applications) are almost impossible to honor because the server does not have direct access to resources on individual workstations.

These products fail to create any balance between static scanning and run-time monitoring. SurfinShield employs run-time monitoring, SurfinGate uses static scanning, and Cage utilizes emulated run-time monitoring. Since static scanning is usually done on

the server and run-time monitoring on the client, this imbalance also causes an imbalance between the load of the server and the client. To distribute the load between the client and the server evenly, the present
5 inventor has determined that a combination of static scanning and run-time monitoring is needed.

SUMMARY

This disclosure is directed to an applet scanner
10 that runs e.g. as an HTTP proxy server and does not require any client-side modification. The scanner combines static scanning and run-time monitoring and does not cause a heavy load on the server. It also does not introduce significant performance overhead
15 during the execution of applets. The scanner provides configurable security policy functionality, and can be deployed as a client-side solution with appropriate modifications.

Thereby in accordance with the invention a scanner
20 (for a virus or other malicious code) provides both static and dynamic scanning for application programs, e.g. Java applets or ActiveX controls. The applets or controls (hereinafter collectively referred to as applets) are conventionally received from e.g. the
25 Internet or an Intranet at a conventional server. At this point the applets are statically scanned at the server by the scanner looking for particular instructions which may be problematic in a security context. The identified problematic instructions are
30 then each instrumented, e.g. special code is inserted

before and after each problematic instruction, where the special code calls respectively a prefilter and a post filter. Alternatively, the instrumentation involves replacing the problematic instruction with
5 another instruction which calls a supplied function.

The instrumented applet is then downloaded from the server to the client (local computer), at which time the applet code is conventionally interpreted by the client web browser and it begins to be executed.
10 As the applet code is executed, each instrumented instruction is monitored by the web browser using a monitor package which is part of the scanner and delivered to the client side. Upon execution, each instrumented instruction is subject to a security
15 check. If the security policy (which has been pre-established) is violated, that particular instruction which violates the security policy is not executed, and instead a report is made and execution continues, if appropriate, with the next instruction.

20 More broadly, the present invention is directed to delivering what is referred to as a "live agent" (e.g., a security monitoring package) along with e.g. an applet that contains suspicious instructions during a network transfer (e.g. downloading to a client), the
25 monitoring package being intended to prevent execution of the suspicious instructions. The suspicious instructions each may (or may not) be instrumented as described above; the instrumentation involves altering suspicious instructions such as by adding code (such as
30 the pre-and post-filter calls) or altering the

suspicious instructions by replacing any suspicious instructions with other instructions.

BRIEF DESCRIPTION OF THE DRAWINGS

5 Fig. 1 shows diagrammatically use of a scanner in accordance with this invention.

 Fig. 2 shows detail of the Fig. 1 scanner.

DETAILED DESCRIPTION

10 Several characteristics of the well known Java language and applets are pertinent to the present scanning method and apparatus. Java is an interpreted, dynamic-linking language. Only the application modules are distributed, and all the standard library functions
15 are provided by the interpreter, for instance a web browser. Because Java byte code is platform-independent, applets have to use some of the standard library functions to access operating system resources.

 This creates two opportunities in accordance with
20 the invention to detect attempts to use operating system resources. First, one can "trick" applets into calling particular functions supplied by the scanner during the dynamic linking stage. This is done by replacing the browser Java library routines with the
25 scanner's monitoring routines of the same name. Second, since invocations of such functions have to be resolved at run-time, symbolic names of these functions are kept in the Java applet module. The scanner can detect possible use of these functions by looking at
30 the static code itself. The first opportunity provides

run-time monitoring. It is the most definitive method to determine the security risks posed by an applet.

The second opportunity enables statically scanning an applet, without running it, to detect possible security risks. If a set of insecure functions is properly defined and an applet never calls any function in the set, the applet can be assumed to be safe. However, this static scanning method is not definitive, since an applet might show different behavior given different user input. Under certain conditions, the instruction in the applet that makes the function call may never be executed. If static scanning is used without run-time monitoring, many such "false alarms" of security risks are produced undesirably.

After the code of an applet is downloaded, e.g. via the Internet to a client platform (local computer), an instance of the applet is created in the conventional Java "virtual machine" in the web browser (client) running on that local computer. Different instances of the same applet might produce different results given different inputs. A running instance of an applet is conventionally called a session; sessions are strictly run-time entities. Static scanning cannot analyze sessions because static scanning does not let the applet run. Sessions are important because an instance of an applet will often perform a series of suspicious tasks before it can be determined dangerous (i.e., in violation of the security policy). Such state information needs to be associated with the sessions. The present applet scanner thereby stops

sessions instead of blocking execution of the entire applet.

A security policy defines what functions an applet needs to perform to be considered a security risk.

5 Examples of security policies include preventing(1) applets from any file access, or (2) file access in a certain directory, or (3) creating certain Java objects. An applet scanner in accordance with the invention may allow different security policies for
10 different clients, for different users, and for applets from different origins.

Fig. 1 is a high level block diagram illustrating the present scanner in the context of conventional elements. The Internet (or an Intranet) is shown
15 generally at 10. The client machine or platform (computer) 14, which is typically a personal computer, is connected to the Internet 10 via a conventional proxy server machine (computer) 20. Client machine 14 also includes local resources 30, e.g. files stored on
20 a disk drive. A conventional web browser 22 is software that is installed on the client machine 14. It is to be understood that each of these elements is complex, but except for the presently disclosed features is conventional.

25 Upon receipt of a particular Java applet, the HTTP proxy server 32, which is software running on server machine 20 and which has associated scanner software 26, then scans the applet and instruments it using an instrumenter 28 which is part of the scanner software
30 26. (Downloaded non-applets are not scanned.) The

instrumented applet is subject to a special digital
signer which is an (optional) part of the scanner 26.
The scanned (instrumented) applet, which has been
digitally signed is then downloaded to the web browser
5 22 in the client 14. The applet is then conventionally
interpreted by the web browser 22 and its instructions
are executed. The execution is monitored by the
monitor package software, also downloaded from scanner
26, in the web browser 22 in accordance with this
10 invention for security purposes. Thus static scanning
is performed by the HTTP proxy server 32 and dynamic
scanning by the web browser 22.

The present applet scanner thus uses applet
instrumentation technology, that is, for Java applets
15 it alters the Java applet byte code sequence during
downloading of the applet to the server 32. After the
Java applet byte code sequence has been downloaded, the
static (pre-run time) scanning is performed on the
applet by the scanner 26. If an instruction (a
20 suspicious instruction) that calls an insecure function
(as determined by a predefined set of such functions)
is found during this static scanning, a first
instruction sequence (pre-filter) is inserted before
that instruction and a second instruction sequence
25 (post-filter) after that instruction by the
instruments.

An example of such a suspicious Java function is
"Java.IO.File.list" which may list the contents of a
client (local) directory 30, e.g. a directory on the
30 client machine 14 hard disk drive. The first

instruction sequence generates a call to a pre-filter function provided by the scanner 26, signaling that an insecure (suspicious) function is to be invoked. The pre-filter checks the security policy associated with the scanner 26 and decides whether this particular instruction ("call") is allowed. The second instruction sequence generates a call to a post-filter function also provided by the scanner. It also reports the result of the call to the post-filter function.

Both the pre- and post-filter functions update the session state to be used by the security policy. The static scanning and instrumentation are both performed on the HTTP proxy server 32.

The following is pseudo-code for the instrumentation process:

```
instrument(JavaClassFile classfile)
{
    extract constant pool from classfile;
    extract functions from classfile;

    for each function
    {
        for each instruction in function
        {
            if( the instruction is a function call
                AND the target of the call is a pre-defined set
                of suspicious functions)
            {
                output an instruction sequence which generates a
                function call to a pre-monitor function, with the
                name of the suspicious function, parameters to the
                suspicious function, and possibly other
                information about his suspicious function
                invocation as the parameters;
```

```
        output the original instruction;

        output an instruction sequence which generates a
        function call to a post-monitor function, with the
5      result of the suspicious function invocation and
        possibly other related information as parameters;
    }
    else
    {
10      output the original instruction;
    }
  }
}

15  Examples of pre- and post-monitor functions are:
    (1) to disallow any directory listing access:
pre-filter(function_name, parameters)
{
    if (function_name == "java.io.File.list")
20  throw new SecurityException();
}

post-filter(result)
{
25  }

    (2) To protect files under c:\temp from directory
    listing access:

pre-filter(function_name, parameters)
30  {
    if
    (function_name == "java.io.File.list")
    {
        extract the name of the file to be read from
35  parameters;
        if the directory to be listed is under c:\temp)
        throw new SecurityException();
    }
}

40  post-filter(result)
    {
    }
```

The pre and post filter and monitoring package security policy functions) are combined with the instrumented applet code in a single JAR (Java archive) file format at the server 32, and downloaded to the web browser 22 in client machine 14. From this point on, the server 32 is virtually disconnected from this server-client session. All the monitoring and applet code is executed in the web browser 22 in the client machine 14. The only time that the server 32 may be again involved during this particular session is when the applet is determined to be dangerous (i.e. including malicious code that violates the security policy) or the applet has completed execution, and a report is sent back to the server 32 by the monitoring code in the scanner 26. A report is optional in this second case.

This approach minimizes the overhead on both server 32 and browser 14. The only work performed on the server 32 is to identify suspicious applet instructions and instrument them, which is usually performed by a one time pass over the applet code. To the client web browser 22, the only overhead is some occasional calls to the scanner monitoring functions, which update session statistics and check security policies. This achieves an optimum distribution of scanning and monitoring between the server 32 and the client web browser 22. Also, the server 32 maintains no state information about active sessions in the set of host associated with the proxy server instead the session state information is maintained locally at

client machine 14 by the downloaded monitoring functions.

This approach may damage the integrity of externally digitally signed (authenticated) applets, since the content of the applets is changed by the instrumentation. However, this can also be used as an advantage because using the present scanner, a new set of authenticated signatures can be set and enforced for the entire domain as further described below.

10 Operation of scanner 26 and its various (software) components is better understood with reference to Fig. 2, showing greater detail than Fig. 1.

 An applet pre-fetcher component 38 fetches from the Internet 10 all the dependency files required by a Java class file, if they are not already packed into a JAR file. This is important because the goal is to attach the scanner monitor package to a session only once.

 A Java applet may contain more than one code module, or class file. Heretofore this disclosure has assumed that all the class files are packed in one JAR file and downloaded once. One monitoring package is attached to the JAR file and every instantiation of this package on the client web browser 22 marks a unique session. However, if the class files are not packed together and are downloaded on an as-needed basis during applet execution, multiple instrumentation will occur and multiple instances of the monitoring package for the same session are created on the client.

30 This creates a problem of how to maintain information

on session states. To solve this problem, the pre-
fetcher 38 pre-fetches the dependency class files
during the static scanning of the main applet code
module. The dependency class files are (see below)
5 instrumented once, packed together, and delivered to
the client.

Upon receiving a (signed) applet, the signal
verifier component 40 then verifies the signature and
its integrity, as conventional, to decide whether to
10 accept this applet.

Next, the unpacker 42 component extracts the class
files from the JAR file. JAR uses ZIP (compression)
format.

Java class parser component 44 then parses each
15 Java class file. Parser 44 conventionally extracts the
instruction sequence of the Java functions.

The Java instrumenter component 48 instruments the
Java class files, e.g. by inserting monitoring
instructions (e.g. pre and post filter calls) before
20 and after each suspicious instruction, as described
above.

The monitor package contains monitoring functions
that are delivered from the server 32 to the client web
browser 22 with the instrumental applet and are invoked
25 by the instrumentation code in the applet. The monitor
package also creates a unique session upon
instantiation. It also contains a security policy
checker (supplied by security policy generator
component 54) to determine whether the applet being

scanned violates the security policy, given the monitoring information.

The security policy generator component 54 generates the security checker code included in the monitor package, from a set of predefined security policies. Different clients, users, and applets may have different security policies. The security policy generator 54 may run on server machine 20 or another computer. In addition, security policies can be configured by an administrator of the system. A simple security policy is to assign different weights to monitored functions and make sure the security weight of a session does not exceed a preset threshold. A more sophisticated security policy checks the file or resource the applet is trying to access at run time and prompts the user whether to allow the access. Hence the security policy broadly is a state machine to detect security policy violations upon attempted instruction execution.

The security policy generator 54 can operate outside the run-time instrumenter component 48 when the security policy is being created. The instrumenter component 48 can then directly use the byte code. Thereby any performance limitations of the security policy generator component 54 become less important.

Next, packer 50 creates a new JAR file (JAR') from the instrumented class files and the monitoring package.

The digital signer component 58 digitally signs the applet (now JAR"), with a digital signature unique

to the particular scanner 26, for authentication in the local domain. The applet JAR" is then transferred to the client machine 14 for execution. Thus the only signature that a client needs to recognize is the
5 digital signature of the signer component 58 in the scanner 26. This pre-verification simplifies system administration and reduces risks to unsophisticated users who might otherwise accidentally accept applets with unauthorized signatures.

10 In one embodiment, the components of scanner 26 are each implemented in Java. Some (or all) of the functions ("components") of the scanner 26 described above may be implemented in native (non-Java) code to improve performance. The actual scanner code is not
15 given here; it can be readily written by one of ordinary skill in the art in light of this disclosure.

This disclosure is illustrative and not limiting, further modifications will be apparent to one skilled in the art and are intended to fall within the scope of
20 the appended claims.

I claim:

1. A method of detecting and preventing
execution of problematic instructions in an application
program provided from a computer network, comprising
5 the steps of:

providing the application program over the
computer network;

determining whether the provided application
program includes any instructions that are members
10 of a particular set of instructions;

executing the application program if it is
determined that no members of the set are included
in the application program;

if it is determined that an instruction is a
15 member of the set, then altering the application
program at the point of the instruction, thereby
allowing monitoring of execution of the
instruction.

20

2. The method of Claim 1, further comprising the
step of associating monitoring code with the
application program.

25 3. The method of Claim 1 wherein the step of
altering includes inserting a first predefined call
before the instruction and a second predefined call
after the instruction.

4. The method of Claim 1, wherein the step of altering includes replacing the instruction with a predefined second instruction.

5 5. The method of Claim 1, wherein the application program is an applet.

6. The method of Claim 2, wherein the applet is in the Java language.

10

7. The method of Claim 1, wherein the computer network is an Intranet or the Internet.

8. The method of Claim 3, wherein the first
15 predefined call is a call to check a security policy.

9. The method of Claim 8, wherein the security policy is a state machine.

20 10. The method of Claim 3, wherein the first or second predefined call changes a session state of the application program.

11. The method of Claim 3, wherein the step of
25 inserting is repeated for each instruction that is a member of the particular set.

12. The method of Claim 1, wherein the particular set of instructions includes instructions that access a
30 predefined set of files.

13. The method of Claim 1, further comprising the steps of:

5 determining if the application program
includes an authentication;
verifying the authentication; and
replacing the verified authentication with a
second authentication.

10 14. The method of Claim 1, further comprising the steps of:

providing all dependency files associated
with the application program;
providing a single monitoring package
15 performing the step of determining for the
application program and its associated dependency
files; and
executing the application program and its
associated dependency files.

20

15. A method of detecting and preventing
execution of problematic instructions in an application
program provided from a computer network, comprising
the steps of:

25 determining if the application program
includes any instructions that are members of a
particular set of instructions;
if any instruction is identified as a member
of the set, associating an agent with the
30 application program; and

transferring the application program with the associated agent to a client for execution.

16. The method of Claim 15, wherein the agent is
5 a monitoring function to prevent execution of members of a particular set of instructions.

17. The method of Claim 15, further comprising the step of instrumenting each of the identified
10 instructions prior to the step of transferring.

18. The method of Claim 15, wherein the computer network is an Intranet or the Internet.

15 19. A scanner for detecting and preventing execution of problematic instructions in an application program provided from a computer network, wherein the scanner determines whether the provided application program includes any instructions that are members of a
20 particular set of instructions, allowing execution of the application program if it is determined that no members of the set are included in the application program; and comprising

an instrumenter which alters the application
25 program at the point of an instruction which is determined to be a member of the set, thereby allowing monitoring of execution of the altered instruction.

30

20. The scanner of Claim 19, further comprising a packer which associates monitoring code with the application program.

5 21. The scanner of Claim 19 wherein the instrumenter inserts a first predefined call before the instruction and a second predefined call after the instruction.

10 22. The scanner of Claim 19, wherein the instrumenter replaces the instruction with a predefined second instruction.

15 23. The scanner of Claim 19, wherein the application program is an applet.

24. The scanner of Claim 20, wherein the applet is in the Java language.

20 25. The scanner of Claim 19, wherein the computer network is an Intranet or the Internet.

25 26. The scanner of Claim 21, wherein the first predefined call is a call to check a security policy.

27. The scanner of Claim 26, wherein the security policy is a state machine.

28. The scanner of Claim 21, wherein the first or second predefined call changes a session state of the application program.

5 29. The scanner of Claim 21, wherein the instrumenter repeats the inserting for each instruction that is a member of the particular set.

10 30. The scanner of Claim 19, wherein the particular set of instructions includes instructions that access a predefined set of files.

15 31. The scanner of Claim 19, further comprising:
 a verifier which determines if the application program includes an authentication and verifies the authentication; and
 a signer which replaces the verified authentication with a second authentication.

20 32. The scanner of Claim 19, further comprising:
 a prefetcher which fetches all dependency files associated with the application program; and
 a security policy generator which provides a single monitoring package for the application
25 program and its associated dependency files.

AMENDED CLAIMS

[received by the International Bureau on 19 January 1999 (19.01.99); original claims 1-4, 6, 11, 13-15, 17, 19, 24 and 29 amended; new claims 33-42 added; remaining claims unchanged (7 pages)]

1. A method of detecting and preventing execution of instructions in an application program provided from a computer network, comprising:

5 providing the application program over the computer network;

determining whether the provided application program includes any instructions that are members of a particular set of instructions;

10 executing the application program if it is determined that no members of the set are included in the application program;

if it is determined that an instruction is a member of the set, then altering the application program, thereby allowing monitoring of execution of the instruction.

2. The method of Claim 1, further comprising associating monitoring code with the application program.

3. The method of Claim 1 wherein the altering includes inserting a first predefined call before the instruction and a second predefined call after the instruction.

4. The method of Claim 1, wherein the altering includes replacing the instruction with a predefined second instruction.

5. The method of Claim 1, wherein the application program is an applet.

6. The method of Claim 5, wherein the applet is in the Java language.

7. The method of Claim 1, wherein the computer network is an Intranet or the Internet.

8. The method of Claim 3, wherein the first predefined call is a call to check a security policy.

9. The method of Claim 8, wherein the security policy is a state machine.

10. The method of Claim 3, wherein the first or second predefined call changes a session state of the application program.

11. The method of Claim 3, wherein the inserting is repeated for each instruction in the application program that is a member of the particular set.

12. The method of Claim 1, wherein the particular set of instructions includes instructions that access a predefined set of files.

13. The method of Claim 1, further comprising:
determining if the application program includes an authentication;
verifying the authentication; and
replacing the verified authentication with a second authentication.

14. The method of Claim 1, further comprising:
providing all dependency files associated with the application program;

providing a single monitoring package
performing the step of determining for the
application program and its associated dependency
files; and

5 executing the application program and its
associated dependency files.

15. A method of detecting and preventing
execution of instructions in an application program
10 provided from a computer network, comprising:
 determining if the application program
includes any instructions that are members of a
particular set of instructions;
 if any instruction is identified as a member
15 of the set, associating an agent with the
application program; and
 transferring the application program with the
associated agent to a client for execution.

20 16. The method of Claim 15, wherein the agent is
a monitoring function to prevent execution of members
of a particular set of instructions.

 17. The method of Claim 15, further comprising
25 instrumenting each of the identified instructions prior
to the step of transferring.

 18. The method of Claim 15, wherein the computer
network is an Intranet or the Internet.

30 19. A scanner for detecting and preventing
execution of instructions in an application program
provided from a computer network, wherein the scanner
determines whether the provided application program

includes any instructions that are members of a particular set of instructions, allowing execution of the application program if it is determined that no members of the set are included in the application

5 program; and comprising:

an instrumenter which alters the application program at an instruction which is determined to be a member of the set, thereby allowing monitoring of execution of such instruction.

10

20. The scanner of Claim 19, further comprising a packer which associates monitoring code with the application program.

15

21. The scanner of Claim 19 wherein the instrumenter inserts a first predefined call before the instruction and a second predefined call after the instruction.

20

22. The scanner of Claim 19, wherein the instrumenter replaces the instruction with a predefined second instruction.

25

23. The scanner of Claim 19, wherein the application program is an applet.

24. The scanner of Claim 23, wherein the applet is in the Java language.

30

25. The scanner of Claim 19, wherein the computer network is an Intranet or the Internet.

26. The scanner of Claim 21, wherein the first predefined call is a call to check a security policy.

27. The scanner of Claim 26, wherein the security
5 policy is a state machine.

28. The scanner of Claim 21, wherein the first or second predefined call changes a session state of the application program.

10

29. The scanner of Claim 21, wherein the instrumenter repeats the inserting for each instruction in the application program that is a member of the particular set.

15

30. The scanner of Claim 19, wherein the particular set of instructions includes instructions that access a predefined set of files.

20

31. The scanner of Claim 19, further comprising:
a verifier which determines if the application program includes an authentication and verifies the authentication; and
a signer which replaces the verified
25 authentication with a second authentication.

25

32. The scanner of Claim 19, further comprising:
a prefetcher which fetches all dependency files associated with the application program; and
30 a security policy generator which provides a single monitoring package for the application program and its associated dependency files.

30

33. The method of Claim 1, wherein the computer network includes a server and a client coupled to the server, and wherein the altering takes place at the server, wherein the executing the application program
5 takes place at the client.

34. The method of Claim 33, further comprising performing the monitoring at the client.

10 35. The method of Claim 1, further comprising carrying out the method of Claim for 1 each of a plurality of application programs as each application program is provided from the computer network.

15 36. The scanner of Claim 19, wherein the computer network includes a server and a client coupled to the server, wherein the altering by the instrumenter takes place at the server, and wherein the executing the application program takes place at the client.

20

37. The scanner of Claim 36, wherein the monitoring is performed at the client.

25 38. The scanner of Claim 19, wherein the instrumenter alters each of a plurality of application programs as each application program is provided from the computer network.

30 39. The method of Claim 1, wherein the instructions are problematic instructions.

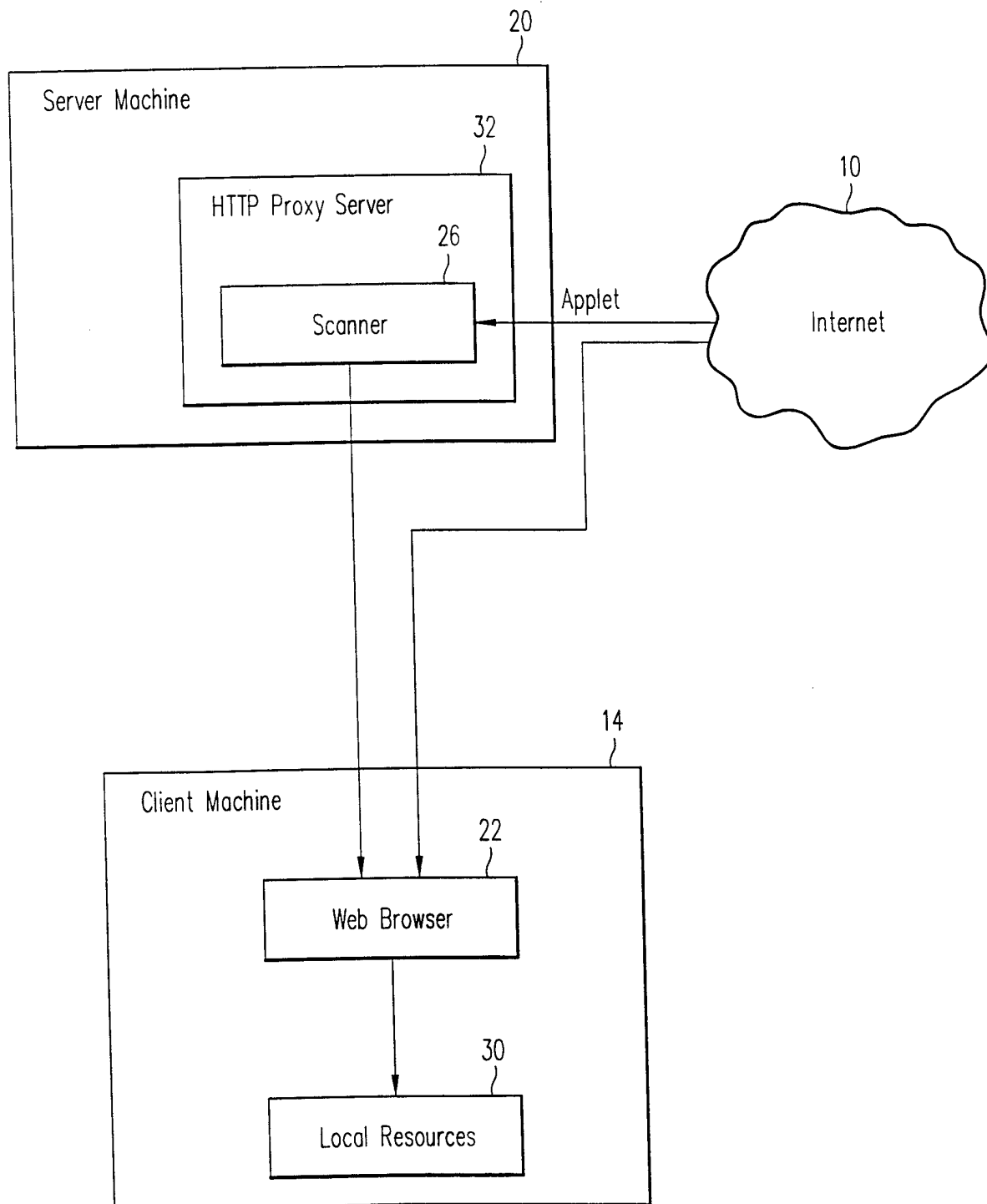
40. The method of Claim 1, wherein the application program is altered at the point of the instruction.

41. The scanner of Claim 19, wherein the instructions that are members of the particular set are problematic instructions.

5

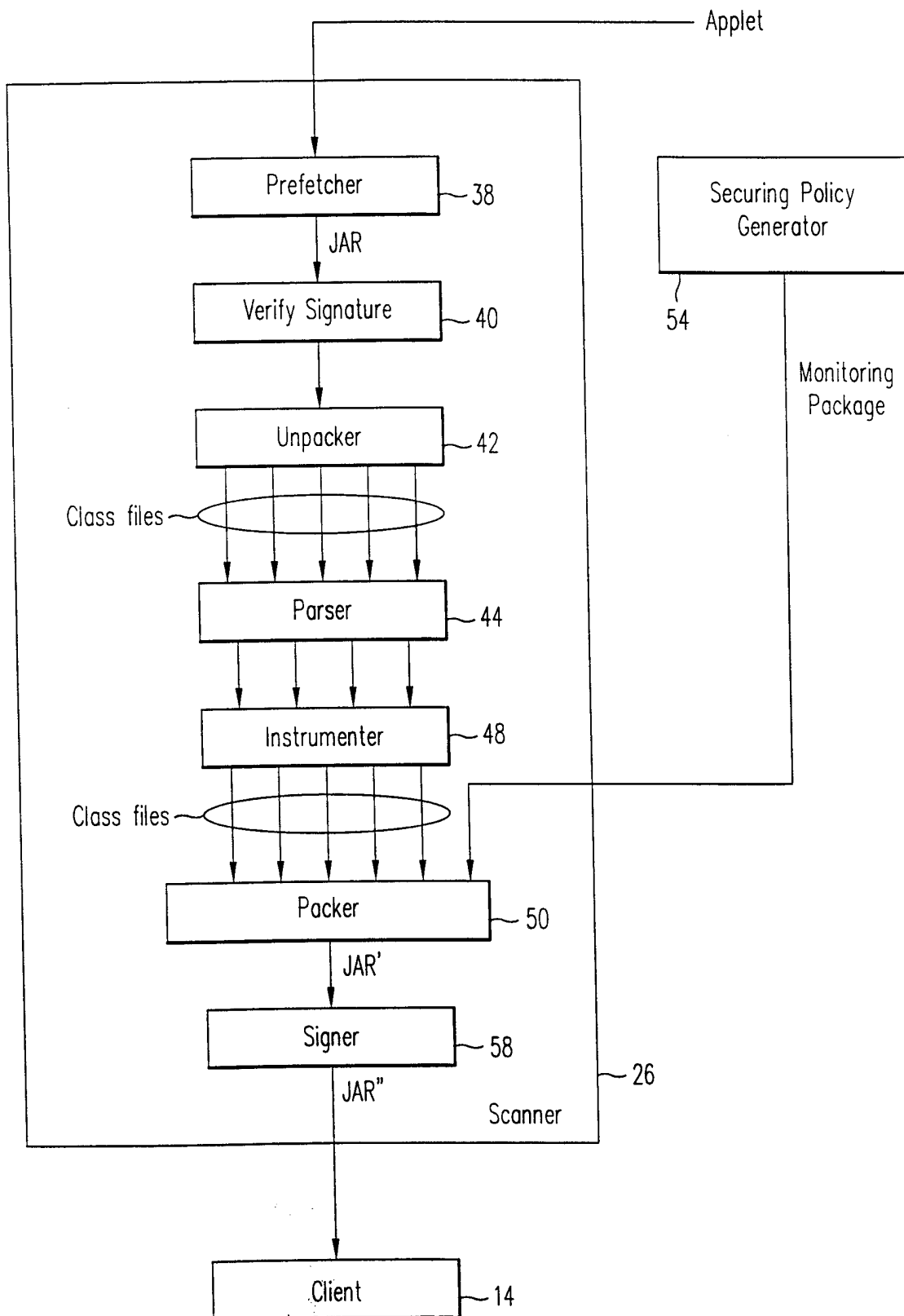
42. The scanner of Claim 19, wherein the alteration is at the point of the instruction.

1/2

**FIG. 1**

SUBSTITUTE SHEET (RULE 26)

2/2

**FIG. 2**

SUBSTITUTE SHEET (RULE 26).

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/15807

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G06F 11/00

US CL : 395/186

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 395/186, 187.01, 188.01, 183.14, 183.13, 200.54, 200.55, 200.32; 380/3, 4, 23, 25

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

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

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,257,381 A (COOK) 26 October 1993, col. 2, lines 10-44, col. 2, line 67 to col. 3, line 14, col. 3, line 31 to col. 5, line 14.	1-9, 11-12, 15-27, 29-30
Y	US 5,623,600 A (JI ET AL) 22 April 1997, col. 2, line 39 to col. 3, line 13, col. 3, line 51 to col. 4, line 15, col. 4, line 56 to col. 5, line 38, col. 5, line 50 to col. 6, line 27, col. 7, line 29 to col. 9, line 26, col. 10, line 26 to col. 11, line 40.	1-9, 11-12, 15-27, 29-30



Further documents are listed in the continuation of Box C.



See patent family annex.

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

Date of the actual completion of the international search

28 SEPTEMBER 1998

Date of mailing of the international search report

02 DEC 1998

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

JOSEPH PALYS

Telephone No. (703) 305-9600

Joni Hill

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/15807

B. FIELDS SEARCHED

Electronic data bases consulted (Name of data base and where practicable terms used):

APS

search terms: virus, scanners, instruction insertions, static or dynamic scanning or monitoring, applets, program downloading, Internet, web browser.