(51) International Patent Classification: G06F 1/00
(21) International Application Number: PCT/US2004/021945
(22) International Filing Date: 8 July 2004 (08.07.2004)
(25) Filing Language: English
(26) Publication Language: English
(30) Priority Data: 60/485,160 8 July 2003 (08.07.2003) US
(71) Applicant (for all designated States except US): SEVENTH KNIGHT® [US/US]; P.O. Box 820808, Vicksburg, MS 39182 (US).
(72) Inventor; and

(54) Title: AUTOMATIC REGENERATION OF COMPUTER FILES DESCRIPTION

Prompt or request a user to identify or specify files and directories for automated file regeneration service to monitor

Verify that the user has provided a backup copy of the monitored files

Initiate one or more instances of automated file regeneration service

Compare all monitored files with a respective backup copy of the monitored files

Yes

No

Any modification of the monitored files and directories detected?

Replace the one or more modified monitored files and directories with the backup copy, if needed, or during computer restart

Store in the registry of the operating system that the automated file regeneration service has replaced one or more modified monitored file or directory

(57) Abstract: A method for regenerating computer files on a computer system having a computer with an operating system, the method includes receiving an input from a user to specify monitored files, detecting modification of at least one of the monitored files, and replacing the at least one modified monitored file with a backup copy of the at least one modified monitored file.
FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

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

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.
AUTOMATIC REGENERATION OF COMPUTER FILES

DESCRIPTION

Related Applications

[001] This non-provisional application is related to and claims priority of Provisional Application No. 60/485,160 filed on July 8, 2003, in the name of Luke KOESTLER, and titled AUTOMATIC REGENERATION OF COMPUTER FILES, the contents of which are fully incorporated herein by reference.

Technical Field

[002] This invention relates to the field of automatic regeneration of computer files.

Background

[003] Computers, and especially network-connected computers, are present in almost every phase of today’s society. Also present, unfortunately, are many types of technological attacks on such computers. Such attacks may come in the form of viruses, worms, Trojan horses, adware, spyware, and others. Although forms of protection, such as anti-virus software using a signature-based techniques, are currently available, there remain many types of threats that are not detected by currently available solutions, even if such solutions are updated on a daily basis. Accordingly, it is desirable to provide methods and apparatus offering increased security to computers and computer systems from known and unknown technological threats.
SUMMARY

[004] Consistent with the invention, systems and methods are provided for regenerating computer files on a computer system having a computer with an operating system. The method includes receiving an input from a user to specify monitored files, automatically detecting modification of at least one of the monitored files, and automatically replacing the at least one modified monitored file with a backup copy of the at least one modified monitored file.

[005] It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the invention, as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[006] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate several embodiments of the invention and together with the description, serve to explain the principles of the invention.

[007] Figure 1 shows a diagram depicting an exemplary computer system in which systems and methods consistent with the principles of the present may be implemented;

[008] Figure 2 shows a flowchart depicting the steps performed by an automatic file regenerator consistent with the principles of the present invention;
[009] Figure 3 shows a flowchart depicting the steps performed by an automatic file regenerator also consistent with the principles of the present invention; and

[010] Figure 4 is a detailed diagram of the automatic file regenerator shown in Figure 1.

DETAILED DESCRIPTION

[011] Reference will now be made in detail to the embodiments consistent with the invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

[012] Consistent with the invention, an automatic file regenerator works in unison with a process authenticator to provide layers of security to protect computer systems. Unlike conventional anti-virus software that must refer to a database of known threats, the process authenticator reverses this process by building a database of known good code, that is, software and scripts approved by the system administrators. A suitable process authenticator is described further in U.S. Patent Application No. 10/252,110, filed September 24, 2002, the contents of which are incorporated by reference herein in their entirety. Any code that has not been approved by an administrator, such as a virus that the anti-virus software could not yet detect, is not allowed to execute on the server or the local computer system. No software is allowed to execute unless specifically approved.
[013] Consistent with the invention, an automatic file regenerator, which provides automatic file regeneration capabilities, is described herein. The automatic file regenerator maintains data integrity of files and data stored in computers. For example, the automatic file generator can ensure data integrity for enterprise servers running critical services that must be available around-the-clock. The automatic file regenerator replaces modified or corrupt data with a fresh copy of the user-approved original. When, for example, an intruder modifies or deletes data from the computer, the automatic file regenerator replaces the data with a fresh copy of the original. In essence, the automatic file regenerator allows a computer to heal itself automatically, time and time again.

[014] Systems and methods consistent with the present invention may be implemented by computers organized in a conventional distributed processing system architecture. Figure 1 is a block diagram illustrating a computer system 100 in which an embodiment consistent with the invention may be implemented. Computer system 100 includes a computer 101 having a bus 102 or other communication mechanism for communicating information, and a processor 104 coupled with bus 102 for processing information. Computer 101 also includes a main memory, such as random access memory (RAM) 106 or other dynamic storage device, coupled to bus 102 for storing information and instructions to be executed by processor 104. RAM 106 also may be used for storing temporary variables or other intermediate information during execution of instructions to be executed by processor 104. During
operation, some or all portions of an operating system 105 are loaded into
RAM 106. Computer 101 further includes a read only memory (ROM) 108 or
other static storage device coupled to bus 102 for storing static information
and instructions for processor 104. A storage device 110, such as a magnetic
disk or optical disk, is provided and coupled to bus 102 for storing information
and instructions. A file system 111 including a plurality of root directories 113
may be stored in storage device 110.

[015] Computer 101 may be coupled via bus 102 to a display 112,
such as a cathode ray tube (CRT), for displaying information to a computer
user. An input device 114, including alphanumeric and other keys, is coupled
to bus 102 for communicating information and command selections to
processor 104. Another type of user input device is cursor control 116, such
as a mouse, a trackball or cursor direction keys for communicating direction
information and command selections to processor 104 and for controlling
cursor movement on display 112. This input device typically has two degrees
of freedom in two axes, a first axis (e.g., x) and a second axis (e.g., y), which
allow the device to specify positions in a plane.

[016] System 100 may further include an input drive device 117, such
as a CD reader, for reading high-capacity computer-readable media, such as
CD-ROMs and CDRs.

[017] The invention is related to the use of computer system 100 for
monitoring and regenerating files on a computer system or network.
According to one implementation, systems and methods consistent with the
present invention collect system information and store it in a central database in response to processor 104 executing one or more sequences of one or more instructions contained in RAM 106. Such instructions may be read into RAM 106 from a computer-readable medium via an input device such as storage device 110. Execution of the sequences of instructions contained in main memory 106 causes processor 104 to perform the process steps described herein. In an alternative implementation, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention. Thus, implementations consistent with the principles of the present invention are not limited to any specific combination of hardware circuitry and software.

[018] The term "computer-readable medium" as used herein refers to any media that participates in providing instructions to processor 104 for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, optical or magnetic disks, such as storage device 110. Volatile media includes dynamic memory, such as main memory 106. Transmission media includes coaxial cables, copper wire and fiber optics, including the wires that comprise bus 102. Transmission media can also take the form of acoustic or light waves, such as those generated during radio-wave and infra-red data communications.

[019] Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, or any other
magnetic medium, a CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, a RAM, PROM, and EPROM, a FLASH-EPROM, any other memory chip or cartridge, a carrier wave as described hereinafter, or any other medium from which a computer can read.

[020] Various forms of computer-readable media may be involved in carrying one or more sequences of one or more instructions to processor 104 for execution. For example, the instructions may initially be carried on the magnetic disk of a remote computer. The remote computer can load the instructions into its dynamic memory and send the instructions over a telephone line using a modem. A modem local to computer system 100 can receive the data on the telephone line and use an infra-red transmitter to convert the data to an infra-red signal. An infra-red detector coupled to bus 102 can receive the data carried in the infra-red signal and place the data on bus 102. Bus 102 carries the data to main memory 106, from which processor 104 retrieves and executes the instructions. The instructions received by main memory 106 may optionally be stored on storage device 110 either before or after execution by processor 104.

[021] Computer 101 also includes a communication interface 118 coupled to bus 102. Communication interface 118 provides a two-way data communication coupling to a network link 120 that is connected to local network 122. For example, communication interface 118 may be an integrated services digital network (ISDN) card or a modem to provide a data
communication connection to a corresponding type of telephone line. As another example, communication interface 118 may be a local area network (LAN) card to provide a data communication connection to a compatible LAN. Wireless links may also be implemented. In any such implementation, communication interface 118 sends and receives electrical, electromagnetic or optical signals that carry digital data streams representing various types of information.

[022] Network link 120 typically provides data communication through one or more networks to other data devices. For example, network link 120 may provide a connection through local network 122 to host computer 124 and/or to data equipment operated by Internet Service Provider (ISP) 126. ISP 126, in turn, provides data communication services through the Internet 128. Local network 122 and Internet 128 both use electric, electromagnetic or optical signals that carry digital data streams. The signals through the various networks and the signals on network link 120 and through communication interface 118, which carry the digital data to and from computer system 100, are exemplary forms of carrier waves transporting the information.

[023] Computer system 100 can send messages and receive data, including program code, through the network(s), network link 120 and communication interface 118. In the Internet example, a server 130 might transmit a requested code for an application program through Internet 128, ISP 126, local network 122 and communication interface 118. Consistent with the present invention, one such downloaded application in the form of an
automatic file regenerator 107 automatically regenerates files on a computer system. The structure of automatic file regenerator 107 is shown in more detail in Figure 4 and will be described below. The received code may be loaded in RAM 106 and executed by processor 104 as it is received. Alternatively, or in addition, it may be stored in storage device 110, or other non-volatile storage for later execution. In this manner, computer system 100 may obtain application code in the form of a carrier wave.

[024] Although computer system 100 is shown in FIG. 1 as being connectable to one server 130, those skilled in the art will recognize that computer system 100 may establish connections to multiple servers on Internet 128. Such servers may include an HTML-based Internet application, which may provide information to computer system 100 upon request in a manner consistent with the present invention.

[025] FIG. 2 and 3 show flowcharts depicting exemplary methods for automatic regeneration of computer files performed by automatic file regenerator 107 (shown in Figure 4) on computer system 100 consistent with the principles of the present invention. A first method (Figure 2) begins by prompting or requesting input from a user, for example, a system administrator, to indicate or specify files and directories for the automatic file regenerator to monitor, step 200. Monitored files may be any type of file, such as but not limited to documents, programs, web pages, and scripts. Monitored files are files that have been specified by the user as read-only files, files that do not change, or system files. In one embodiment, monitored
files are stored in one or more root directories. The method may verify that
the user has provided a backup copy of the monitored files, step 205. If a
computer running the automatic file regenerator detects that a monitored file
has been modified, renamed, or deleted, then the monitored file is replaced
with the backup copy of the original, usually within seconds. In some
instances the modified monitored file is replaced when the computer is
restarted.

[026] In one configuration, a service initiator 402 (Figure 4) initiates an
instance of automatic file regeneration service for each root directory specified
by the user, step 210. The automatic file regeneration service may be a low-
level system service. The service activates a file comparator 404 to detect
any modification of the monitored files by comparing attributes such as file
size, file name, and binary file composition of the monitored files against the
backup copy of the monitored files, step 220. The automatic file regeneration
service cycles through and compares all monitored files with the respective
backup copy once every cycle. The length of a cycle is set or turned off using
a registry value where, for example, 0 = off, 1 = 1 minute, 2 = 2 minutes, etc.
If the service detects modification of any of the monitored files, step 230, it
replaces the modified monitored files with a backup copy of the original, step
240.

[027] Once the automatic file regeneration service replaces modified
monitored files with a backup copy of the original, the service records an entry
in a registry 103 of operating system 105, step 250. Each service record may
indicate the name of the replaced files, time when the service detected the
modification, time when the service replaced the modified files, and other
information.

[028] The process between steps 220-250 is repeated until the user
stops the automatic file regenerator, turns off the computer, or otherwise
indicates a desire to terminate the process.

[029] A second method consistent with the invention is shown in
Figure 3. The method first prompts or requests input from a user, for
example, a system administrator, to indicate or specify files and directories for
the automatic file regenerator to monitor, step 300. The method may verify
that the user has provided a backup copy of the monitored files, step 305.
The method then registers the automatic file regeneration service as a file-
system object, step 310. A message requestor 408 requests a copy of any
file change messages sent by the operating system 105 for any directories
and sub-directories within the root directory specified by the user for the
instance of the file regeneration service, step 320. For example, the system
may audit information from monitored file systems or directories using the
processes and method described in U.S. Patent Application No. 10/216,917,
filed August 13, 2002, entitled "Auditing Computer System Components in a
Network," the contents of which are incorporated by reference herein in their
entirety. If the service receives a message of modification of any of the
monitored files, step 330, it replaces the modified monitored files with a
backup copy of the original, step 340.
[030] Once the automatic file regeneration service replaces modified monitored files with a backup copy of the original, the service records an entry in the registry of operating system 105, step 350. Each service record may indicate the name of the replaced files, time when the service detected the modification, time when the service replaced the modified files, and other information.

[031] The process between steps 320-350 is repeated until the user stops the automatic file regenerator, turn off the computer, or otherwise indicates a desire to terminate the process.

[032] The automatic file regenerator cannot replace files that are marked as "in use" or locked by the operating system 105 or another program. However, in most cases these files are replaced as soon as the operating system 105 or the other program releases the "in use" status of the modified files. It is important to note that the system or the local system account must possess full rights to the monitored files and read-only rights to the backup copy of the monitored files. Preferably, the automatic file regenerator uses read-only media, such as a CD-ROM or CDR, to store backup copies of the monitored files. Alternatively, the automatic file regenerator may store the backup copy on another server 124 or 130, on device 110, or on any computer-readable medium.

[033] Both methods of detecting file modification require no user interaction, and only replace files that have been modified or removed. The methods use no resources of computer 101 unless the automatic file
regenerator is actively restoring a file or directory. One of ordinary skill in the art will recognize that the configurations described above are embodiments of the present invention, and other configurations may be practiced in a manner consistent with the principles of the present invention,

[034] Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.
WHAT IS CLAIMED IS:

1. A method for regenerating computer files on a computer system including a computer with an operating system, comprising:
   receiving an input from a user to specify monitored files;
   detecting modification of at least one of the monitored files; and
   replacing the at least one modified monitored file with a backup copy of
the at least one modified monitored file.

2. The method of claim 1, comprising:
   initiating an instance of automatic file regeneration service, after
receiving user input.

3. The method of claim 2, wherein the detecting further comprises:
   comparing the monitored files with a respective backup copy of the
monitored files.

4. The method of claim 3, wherein the comparing comprises:
   comparing the monitored files with a respective backup copy of the
monitored files by comparing the attributes of the monitored files and their
respective backup copy.

5. The method of claim 4, comprising:
   storing an indication in a computer operating system registry when the
automatic file regeneration service replaces the at least one modified
monitored file.

6. The method of claim 4, wherein the monitored files are stored in at
least one root directory specified by the user.
7. The method of claim 6, wherein the initiating comprises:
initiating an instance of automatic file regeneration service for the at least one root directory.

8. The method of claim 7, comprising:
storing an indication in a computer operating system registry when the automatic file regeneration service replaces the at least one modified monitored file.

9. The method of claim 8, wherein the replacing comprises replacing on a real-time basis.

10. The method of claim 8, wherein the replacing is performed when the computer is restarted.

11. The method of claim 1, comprising:
registering automatic file regeneration service as a file-system object of the operating system, after receiving user input.

12. The method of claim 11, wherein detecting further comprises:
requesting a copy of any file change messages sent by the operating system.

13. The method of claim 12, wherein the operating system comprises a registry and the method comprises:
storing an indication in the registry that the automatic file regeneration service has replaced at least one modified monitored file.

14. The method of claim 13, wherein the monitored files are stored in root directories specified by the user.
15. The method of claim 14, wherein the replacing comprises replacing on a real-time basis.

16. The method of claim 14, wherein the replacing is performed when the computer is restarted.

17. A system for regenerating computer files on a computer system including a computer with an operating system, comprising:
   an input receiving unit operable to receive an input from a user to specify monitored files; and
   a file regenerator operable to detect modification of at least one of the monitored files and replace the at least one modified monitored file with a backup copy of the at least one modified monitored file.

18. The system of claim 17, comprising:
   a service initiator operable to initiate an instance of automatic file regeneration service.

19. The system of claim 18, wherein the file monitor further comprises:
   a file comparator operable to compare the monitored files with a respective backup copy of the monitored files.

20. The system of claim 19, wherein the file regenerator further compares the monitored files with a respective backup copy of the monitored files by comparing the attributes of the monitored files and their respective backup copy.

21. The system of claim 20, comprising:
a computer registry operable to store an indication in a computer operating system registry when the automatic file regeneration service replaces the at least one modified monitored file.

22. The system of claim 20, wherein the monitored files are stored in at least one root directory specified by the user.

23. The system of claim 22, wherein the service initiator further initiates an instance of automatic file regeneration service for the at least one root directory.

24. The system of claim 23, comprising:

a computer registry operable to store an indication in a computer operating system registry when the automatic file regeneration service replaces the at least one modified monitored file.

25. The system of claim 24, wherein the automatic file regeneration service replaces the at least one modified monitored file on a real-time basis.

26. The system of claim 24, wherein the automatic file regeneration service replaces the at least one modified monitored file when the computer is restarted.

27. The system of claim 17, comprising:

a service register operable to register automatic file regenerating service as a file-system object of the operating system.

28. The system of claim 27, wherein the step of detecting further comprises: a message requestor operable to request a copy of any file change messages sent by the operating system.
29. The system of claim 28, further comprising:

a computer registry operable to store an indication in the registry that
the automatic file regeneration service has replaced at least one modified
monitored file.

30. The system of claim 29, wherein the file regenerator replaces the at
least one modified monitored files on a real-time basis.

31. The system of claim 29, wherein the file regenerator replaces the at
least one modified monitored files when the computer is restarted.

32. A computer-readable medium containing instructions for performing
a process for regenerating computer files on a computer system including a
computer with an operating system, the process comprising:

receiving an input from a user to specify monitored files;

detecting modification of at least one of the monitored files; and

replacing the at least one modified monitored file with a backup copy of
the at least one modified monitored file.

33. The computer-readable medium of claim 32, comprising:

initiating an instance of automatic file regeneration service, after
receiving user input.

34. The computer-readable medium of claim 33, wherein the step of
detecting further comprises:

comparing the monitored files with a respective backup copy of the
monitored files.
35. The computer-readable medium of claim 38, wherein the step of comparing comprises:

comparing the monitored files with a respective backup copy of the monitored files by comparing the attributes of the monitored files and their respective backup copy.

36. The computer-readable medium of claim 35, comprising:

storing an indication in a computer operating system registry when the automatic file regeneration service replaces the at least one modified monitored file.

37. The computer-readable medium of claim 35, wherein the monitored files are stored in at least one root directory specified by the user.

38. The computer-readable medium of claim 37, wherein the step of initiating comprises:

initiating an instance of automatic file regeneration service for the at least one root directory.

39. The computer-readable medium of claim 38, comprising:

storing an indication in a computer operating system registry when the automatic file regeneration service replaces the at least one modified monitored file.

40. The computer-readable medium of claim 39, wherein the replacing comprises replacing on a real-time basis.

41. The computer-readable medium of claim 39, wherein the replacing is performed when the computer is restarted.
42. The computer-readable medium of claim 32, comprising:
registering automatic file regeneration service as a file-system object of
the operating system, after receiving user input.

43. The computer-readable medium of claim 42, wherein the step of
detecting further comprises:
requesting a copy of any file change messages sent by the operating
system.

44. The computer-readable medium of claim 43, comprising:
storing an indication in the registry that the automatic file regeneration
service has replaced at least one modified monitored file.

45. The computer-readable medium of claim 44, wherein the monitored
files are stored in root directories specified by the user.

46. The computer-readable medium of claim 45, wherein the replacing
comprises replacing on a real-time basis.

47. The computer-readable medium of claim 45, wherein the replacing
is performed when the computer is restarted.

48. An apparatus for regenerating computer files on a computer system
including a computer with an operating system, comprising:
means for receiving an input from a user to specify monitored files,
wherein the monitored files are stored in at least one root directory specified
by the user;
means for initiating an instance of automatic file regeneration service,
after receiving user input;
means for detecting modification of at least one of the monitored files by comparing the monitored files with a respective backup copy of the monitored files; and

means for replacing the at least one modified monitored file with a backup copy of the at least one modified monitored file.
Prompt or request a user to indicate or specify files and directories for automated file regeneration service to monitor

200

Verify that the user has provided a backup copy of the monitored files

205

Initiate one or more instances of automated file regeneration service

210

Compare all monitored files with a respective backup copy of the monitored files

220

Continue?

Yes

Any modification of the monitored files and directories detected?

230

No

Replace the one or more modified monitored files and directories with the backup copy, in real-time or during computer restart

240

Store in the registry of the operating system that the automated file regeneration service has replaced one or more modified monitored file or directory

250

FIG. 2
Prompt or request a user to indicate or specify files and directories for automated file regeneration service to monitor

Verify that the user has provided a backup copy of the monitored files

Register an automated file regeneration service as a file-system object

Request a copy of any file change messages sent by operating system for any monitored files and directories

Continue?

Yes

Any modification of the monitored files and directories detected?

No

Replace the one or more modified monitored files and directories with the backup copy, in real-time or during computer restart

Store in the registry of the operating system that the automated file regeneration service has replaced one or more modified monitored file or directory

FIG. 3
Service Initiator 402
File Comparator 404
Message Requestor 406
**INTERNATIONAL SEARCH REPORT**

**A. CLASSIFICATION OF SUBJECT MATTER**

IPC 7 G06F1/00

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

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06G G06F

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

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

EPO-Internal

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 2002/073106 A1 (LEIGNER GARY J ET AL)</td>
<td>1-48</td>
</tr>
<tr>
<td></td>
<td>13 June 2002 (2002-06-13) page 1, paragraph 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>page 1, paragraph 9 - page 2, paragraph 23</td>
<td></td>
</tr>
<tr>
<td></td>
<td>page 4, paragraph 98 - page 5, paragraph 131</td>
<td></td>
</tr>
<tr>
<td></td>
<td>page 6, paragraph 152 - paragraph 155</td>
<td></td>
</tr>
<tr>
<td></td>
<td>page 7, paragraph 187 - paragraph 195</td>
<td></td>
</tr>
<tr>
<td></td>
<td>page 8, paragraph 200 - paragraph 202</td>
<td></td>
</tr>
<tr>
<td></td>
<td>claim 1</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>WILLIAMS R N: &quot;DATA INTEGRITY WITH VERACITY&quot;</td>
<td>1-48</td>
</tr>
<tr>
<td></td>
<td>INTERNET CITATION, 12 September 1994 (1994-09-12),</td>
<td></td>
</tr>
<tr>
<td></td>
<td>XP002096828</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the whole document</td>
<td></td>
</tr>
</tbody>
</table>

Further documents are listed in the continuation of box C.

Patient family members are listed in annex.

**Date of the actual completion of the international search**

27 December 2004

**Date of mailing of the international search report**

07/01/2005

Name and mailing address of the ISA

European Patent Office, P B. 5818 Patentlaan 2
NL - 2280 HV Hilversum
Tel (+31-70) 340-2040, Tx 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer

Arbutina, L
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>US 6 275 942 B1 (LETSINGER RICHARD ET AL) 14 August 2001 (2001-08-14) column 9, line 58 - column 10, line 61</td>
<td>1,17,32</td>
</tr>
<tr>
<td>A</td>
<td>MCKOSKY R A ET AL: &quot;A FILE INTEGRITY CHECKING SYSTEM TO DETECT AND RECOVER FROM PROGRAMMODIFICATION ATTACKS IN MULTI-USER COMPUTER SYSTEMS&quot; COMPUTERS &amp; SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 9, no. 5, 1 August 1990 (1990-08-01), pages 431-446, XP000147838 ISSN: 0167-4048 the whole document</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>WO 03/021402 A (DUKE DAVID JOHN; CRYPTIC SOFTWARE LTD (GB)) 13 March 2003 (2003-03-13) page 1, line 21 - line 27 page 5, line 9 - page 6, line 4</td>
<td></td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 7123800 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AU 7357200 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0118715 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 0118717 A1</td>
</tr>
<tr>
<td>US 6275942 B1</td>
<td>14-08-2001</td>
<td>AU 7586998 A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2002161908 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2002157089 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2002087883 A1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>US 2002091763 A1</td>
</tr>
</tbody>
</table>