

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
13 March 2003 (13.03.2003)

PCT

(10) International Publication Number
WO 03/021402 A2

(51) International Patent Classification⁷: **G06F 1/00**

(21) International Application Number: PCT/GB02/04059

(22) International Filing Date:
5 September 2002 (05.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0121497.2 5 September 2001 (05.09.2001) GB

(71) Applicant (for all designated States except US): **CRYPTIC SOFTWARE LIMITED** [GB/GB]; The Business Exchange, Rockingham Road, Kettering, Northants NN16 8JX (GB).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **DUKE, David, John** [GB/GB]; 3 The Saplings, Kettering, Northants NN16 9UL (GB).

(74) Agent: **CRAWFORD, Andrew, B.**; AA Thornton & Co., 235 High Holborn, London WC1V 7LE (GB).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report

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.

(54) Title: NETWORK SECURITY

(57) Abstract: A computer network comprises a server computer and a plurality of local computers. Each local computer is provided with an engine program which monitors all files and peripherals and detects changes in the files or configuration. The results of the monitoring are used to create compressed information relating to the files and peripherals which is communicated to the server computer which stores previous information relating to the files and peripherals of the local computers. The server computer compares the received information with the stored information in order to detect the presence of altered and unwanted files or changes in configuration. In this way both known and unknown viruses can be detected as can un-authorised use of the local computers.



WO 03/021402 A2

NETWORK SECURITY

The present invention relates to an arrangement for monitoring the security of a computer especially computers on a network and particularly individual
5 devices and information contained therein.

It is well known to provide individual computers with virus checking software but it is also well known that such software consumes resources when it is run and also takes time. Additionally, updating such software is somewhat cumbersome as each individual computer has to be updated separately.

10 Further, it is known to provide firewalls to protect computers and computer systems which are connected to a network or to the outside world but again these firewalls have limitations and they do not provide a completely effective defence to potential hackers.

Both of these methodologies are reactive and only detect threats to a
15 network which have been seen and indexed previously.

It is an object of the present invention to provide an arrangement whereby protection from attack by viruses is improved as well as providing a more effective firewall in the event that the computer or computer system is provided with such. It is a further object that the invention is deployed in such a way that it
20 is itself not vulnerable to attack.

From one aspect, the present invention is based on a concept whereby a main memory holds a record of all files used by a local computer, is provided with update information on all existing files as well as all new files and determines whether the updated files or new files represent a security threat.

25 In a preferred embodiment, as data is created, modified or deleted on the local computer, events are monitored and collected by an engine program and forwarded to the main memory. Preferably, the engine program itself consists of a

single file which is arranged to run a program in parallel with the normal operating system of the local computer thus making the file easier to hide so that the presence of the engine program will not be noticed either by the user or by a hacker. Further, as far as the user of the local computer is concerned, the engine
5 program has no noticeable effect on the system. Preferably, the main memory is provided by a central computer (hereafter referred to as the console) and the local computer communicates with the console over a network or in some other convenient manner.

The engine program monitors each and every file and by inspecting
10 preselected parts of each file can create a highly compressed accurate image of the file which can then be transmitted to the central database. It will be appreciated that all files can be handled in this way. Consequently, when the term "file" is used we mean all files associated with the operating system, data, registries, directories, hardware, software and such like. In this way, a complete virtual
15 image of a local computer can be stored within the central database and the console can have management software for monitoring changes in the data files, programs or hardware of the local computer and thus warn of tampering with such files, programs and/or hardware.

From another aspect, the present invention provides a method of
20 monitoring the security of a computer system comprising monitoring a file as it is created or updated by inspecting preselected portions of the file selected from the whole file, storing information derived from the preselected portions and transmitting the stored information to a main memory location. The main memory location is preferably a central database of a network.

25 From a further aspect the present invention provides a method of improving the security of computer apparatus by providing two copies of a security program and interconnecting them such that as one is switched off, either deliberately or

inadvertently, the other is automatically switched on and vice versa. It is to be understood that this aspect is not limited to any particular type of security program and is of general application. However, it has particular application with the present invention where the security program is relatively small and easy to hide.

5 In order that the present invention be more readily understood, an embodiment thereof will now be described with reference to the accompanying drawings in which: -

Fig 1 shows a block diagram of a network according to the present invention;

10 Fig 2 shows a block diagram representing the main functions of an engine program arranged to be installed on each computer to be protected; and

Fig 3 is a flow chart for explaining the operation of the engine program of Fig 1.

The present invention will be described in relation to its use for network security but it will be appreciated that the invention can be implemented in a number of different ways independently of any connection technology. In fact, the totality of the invention could be located within a single computer or a local computer could be in communication with a central server over conventional telephone lines rather than utilising any network protocol.

20 As shown in Fig 1, a central server 1 communicates via transmit/receive ports 2 with a number of local computers 3, each of which is provided with a monitoring engine program 4. The central server is provided with a plurality of databases, namely an archive of threats database 5, a virtual image of each computer database 6 and an audit database 7.

25 The basis of the present embodiment is that a virtual copy of a local computer and all its files will be kept in memory at the database to the central server computer with each file having its own individual characteristics stored at

the central computer. The virtual copies are created by the small engine programs 4 loaded on the local computers 3 which monitor all files by inspecting preselected portions of the files in order to create a so-called "fingerprint" of each file which is in fact a highly compressed version of the file. The fingerprint can then be very speedily forwarded to the central location where the current fingerprint can be compared with a previous fingerprint and any changes detected. The changes are then evaluated by the central computer 1 in order to determine the level of threat, if any, to the security of the local computer system and an appropriate signal sent back from the central server to the local computer 3 in the event that a particular file should not be opened or a particular program should not be run. Simultaneously, an event is displayed at the central computer and/or forwarded to other programs.

It will be appreciated that by the use of a virtual copy of the local computer and all its files, the central server can then monitor and log all changes to files, programs and/or hardware in order to provide evidence of breaches of security at the local computer. As an example of this, one could consider a computer fitted with several pieces of memory. Removal of all or part of this memory is an event which can be detected by the engine program and thus signalled to the central computer which can log the event.

In further explanation of the evidential facilities of this invention on the triggering of specified events, biometric information can be gathered in real time and forwarded to the central database. For example, if an event is detected, a screen shot of the local computer is gathered for evidence and at the same time the engine program can gather biometric information such as a photograph of the user of the local computer.

The above description represents a simple brief overall view of the arrangement in accordance with the present invention but for a more detailed

description we will now separate the operation of the engine program at the local computer and firstly describe this before we move onto a description of the operation of the monitoring program at the central server.

The engine program is shown diagrammatically in Fig 2 where all file data
5 is monitored at monitoring section 11 under the control of a program section 12 which determines which parts of the data will be sampled. The selected parts of the data are then stored as indicated at 14 in order to create a virtual compressed copy of the file data for transmission as indicated at 16.

The engine program is arranged to commence running as soon as the
10 computer on which it is loaded is powered up. The program then monitors all files as they are opened and in particular it monitors all changes to a file as indicated by the flow chart shown in Fig 3. Each and every change is inspected in order to determine whether the change is the creation of a new file. It also determines whether the change is a valid change. Each file is also checked by inspecting the
15 file from a plurality of points of view by sampling predetermined portions of the file. This in turn creates a fingerprint or virtual copy of the file which is then assembled for transmission to a central database either over the network or via some other communications link. Among the predetermined portions of the file which the engine program inspects is the tag indicating whether or not the file is
20 an executable. It also determines whether the file is a manipulated file, eg a zipped or encrypted file. It looks for the presence of capabilities such as keystroke logging, FTP server capability, IP notification, joystick controls, game libraries, etc

The engine program has a memory capability 12 so that it can store
25 instructions received from the central processor as described below and then carry out those instructions in the event that the fingerprint it has assembled of a file indicates that action is necessary. As an example, if a known threat is present in a

file as indicated by the fingerprint, the engine program can immediately kill the threat in view of the fact that it has the necessary instruction previously received from the central server. In certain circumstances, the file in question can be automatically dealt with.

5 A particular feature of the engine program is that it does not wait to be polled by a central computer. Rather, it itself generates a message for transmission to the central computer. This has the advantage that the engine program is immune to attack from a hacker because there is no "listening" port waiting for an incoming transmission. It is not until the engine program has
10 communicated with the central server that a two way communication is possible and only after the engine program's communication with the central server can the central server transmit modified information to the engine program. However, the monitoring and modification of the files on the local computer occur in real time while the local computer is in operation either by being started up or while the
15 local computer is running programs. Further, the engine program can itself run other software in order to transmit and/or record data as a result of the detection of a particular event or change to a file. As an example of this, if the local computer is fitted with a web cam, should particular files be modified, the engine program can take a picture of the user of the machine at the appropriate time and correlate
20 the event with the actual user as evidence for subsequent use.

 In an especially secure system, it is possible to provide two identical engine programs which are interlinked with each other so that in the event that one is disabled for any reason, eg being switched off, the other is activated before the first is terminated and vice versa. This ensures security in the event that one of the
25 engine programs is detected by a hacker or other person seeking to tamper with the local computer.

Turning now to the central server 1, this contains a reception port 2 for receiving data transmitted from the local computer. As fingerprints are stored, the central computer builds up a virtual picture of each local computer, its hardware, programs and files generally in its database 6. In addition, the central server
5 maintains a database 5 of all known security threats and viruses. As fingerprints of files are received these are compared with the information in the threats database 5 so that any threat can be detected instantaneously. Additionally, because the central server maintains an up to date virtual copy of each local computer with which it is in communication, in the event that it identifies a
10 security threat in relation to one computer 3, it can then inspect all other local computers for similar configurations and then be ready to communicate the necessary instruction to another local computer 3 as soon as the other local computer communicates with the central server for any reason. In this way, security threats and the mechanism of deleting files or repairing infected files can
15 be undertaken much more quickly and in fact even before a local computer might have been subjected to attack or infection. In other words, when a new threat is identified, it is added to the server database so that the central processor can check its data relating to the local computers to which it is connected or identify other infected systems without the need to communicate with them. Therefore even if a
20 laptop is disconnected or machines are powered down, threats can still be identified and remedial action taken once such machines are back in communication with the central server.

In the same way, the central computer can monitor changes to hardware and software using the information in the database 7 and consequently know when a
25 security breach might have taken place. In this case, the central computer can log the event in question or signal the local computer to take the necessary action to

provide evidence of the possible security breach, eg by taking a web cam picture as well as recording the user name and password.

Another sophisticated ability of the server is to construct a dynamic accurate focused detection formula which can be custom built to detect dynamic
5 changing threats which avoid typical security fingerprinting techniques.

The central server can communicate back to the local computer in the event of a security breach or potential security breach or it can communicate with some other communications device such as a mobile telephone or personal digital assistant by sending an e-mail SMS or fax to indicate the existence of the security
10 breach or potential security breach. In this way, users of portable computers could be warned of security breaches relating to their machine without the need to actually switch it on and establish communications with the central server.

CLAIMS:

1. A computer arrangement comprising a central processor, first memory means for storing an operating system program for the central processor, further
5 memory means for storing data relating to all files used by the computer arrangement, storage means separate from the first storage memory means for storing an engine program for monitoring files used or created by the computer arrangement, and means for communicating the results of the monitoring to the further memory means.
- 10 2. A computer arrangement according to claim 1, wherein the engine program is arranged to inspect preselected parts of each file and create a compressed version of the file.
- 15 3. A computer arrangement according to claim 1, wherein the further memory means is located remote from the central processor and first memory means.
4. A computer arrangement according to claim 3, wherein the means for communicating results to the further memory means comprises a network
20 connection.
5. A computer arrangement according to claim 1, wherein the storage means is arranged to store two engine programs each of which is capable of being switched off and which are interconnected such that as one is switched off, the
25 other is switched on.

6. A computer arrangement according to claim 1, wherein the engine program is arranged to monitor peripheral devices connected to the arrangement in order to detect the presence of new devices and the absence of previously connected devices.

5

7. A computer arrangement according to claim 6, wherein the engine program is arranged to record data relating to any change in peripheral devices or files.

8. A computer arrangement according to claim 3, wherein the further memory means is located in a further computer which is arranged to analyse the results of the monitoring.

10

9. A computer arrangement according to claim 8, wherein the further computer is arranged to transmit instructions to the central processor depending on the results of the analysis.

15

1/2

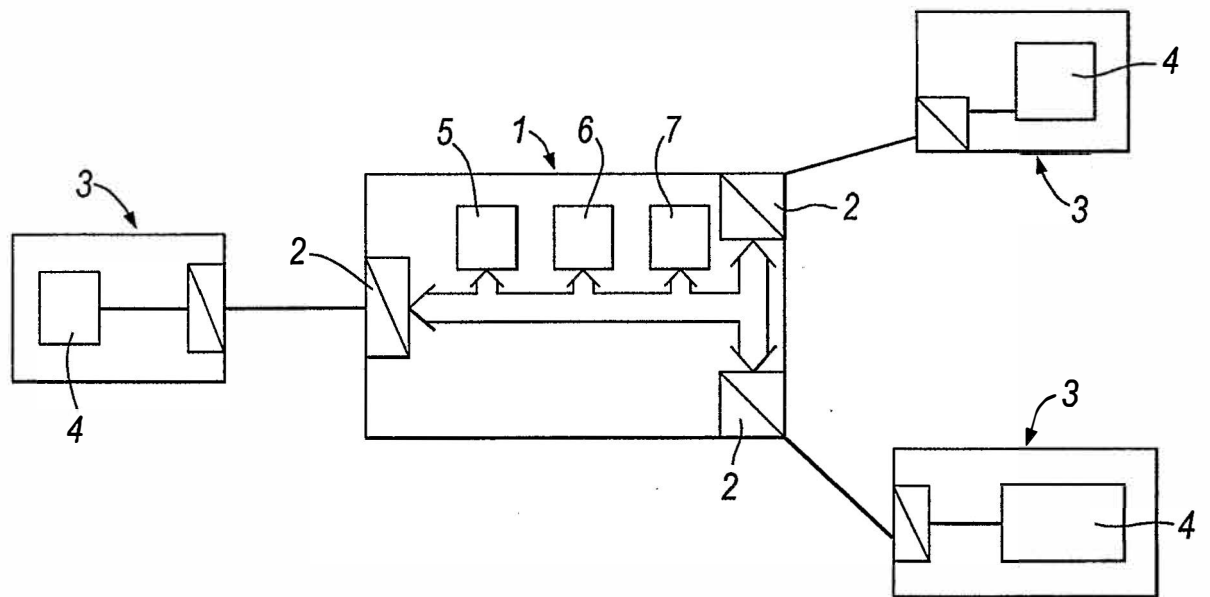


Fig. 1

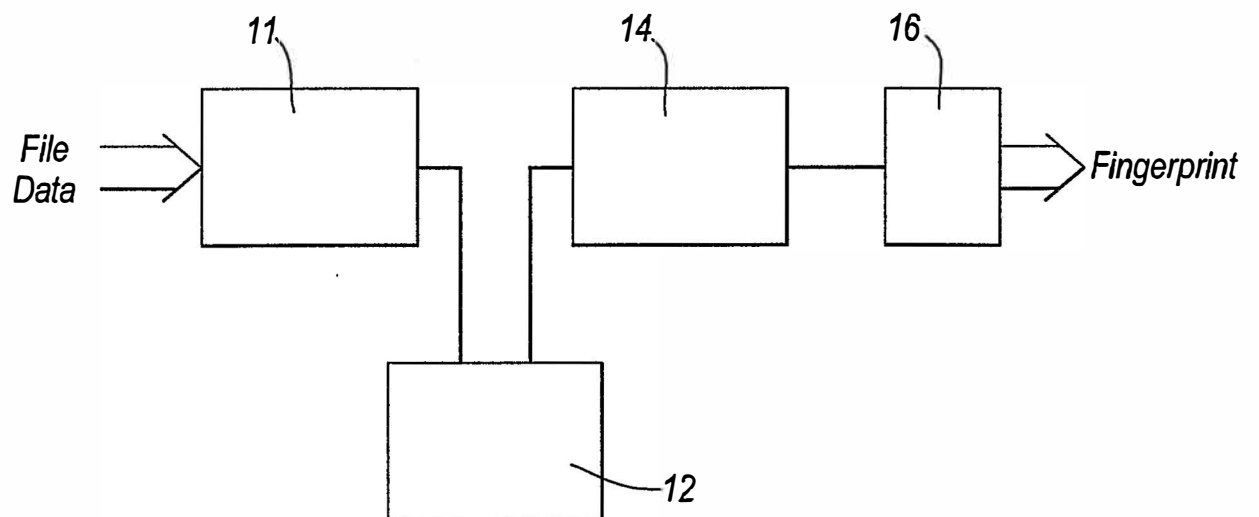


Fig. 2

2/2

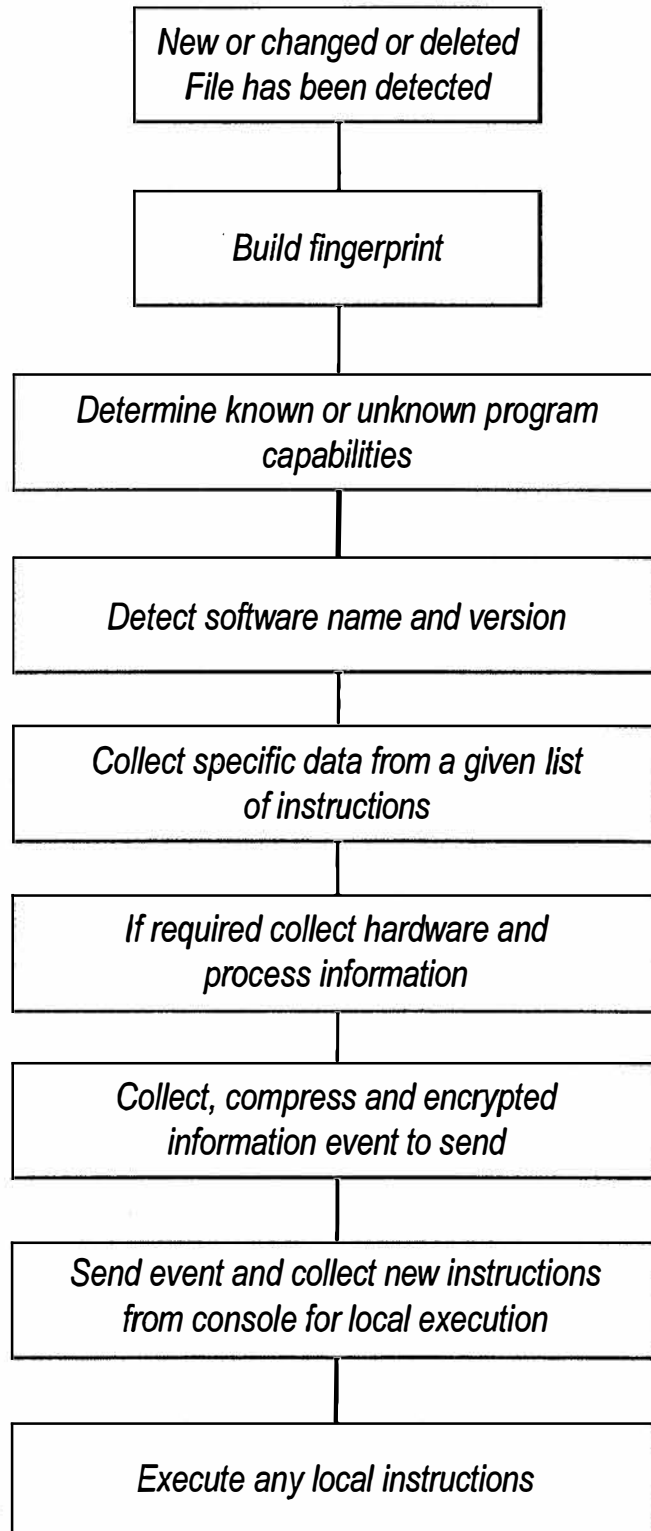


Fig.3