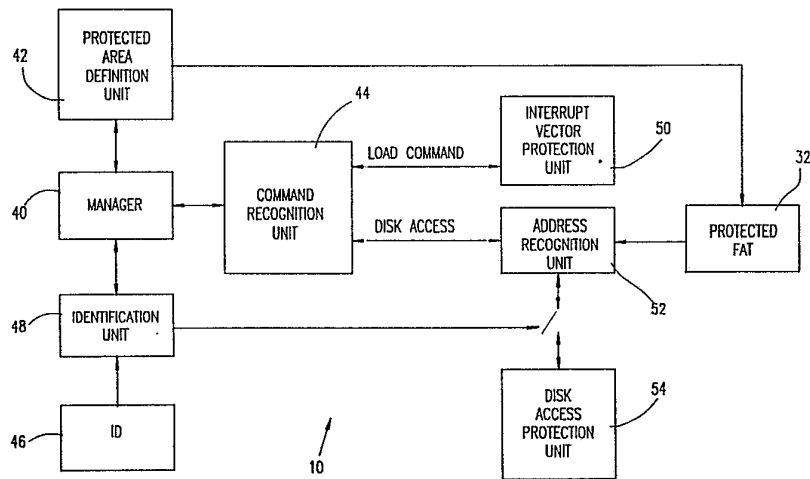




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁵ : G06F 9/06, 15/24</p>	<p>A1</p>	<p>(11) International Publication Number: WO 93/13477 (43) International Publication Date: 8 July 1993 (08.07.93)</p>
<p>(21) International Application Number: PCT/US92/11374 (22) International Filing Date: 23 December 1992 (23.12.92) (30) Priority data: 07/812,733 23 December 1991 (23.12.91) US (71) Applicant: ONYX TECHNOLOGIES (USA) INC. [US/US]; 19-03 Maple Avenue, Fairlawn, NJ 07410 (US). (72) Inventors: KEDMI, Shmuel, Y. ; 17 Balfour Street, 92 102 Jerusalem (IL). LENGER, Eliahu, Dror ; 10 Massat Moshe Street, 93 710 Jerusalem (IL). (74) Agent: MASON, Dennis, A.; Abelman Frayne & Schwab, 708 Third Avenue, New York, NY 10017 (US).</p>		<p>(81) Designated States: CA, JP, KR, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published <i>With international search report.</i></p>

(54) Title: COMPUTER PROTECTION DEVICE



(57) Abstract

An apparatus (10) for protecting access to at least one area of a disk includes an identification unit (48), a manager (40), a protection area definition unit (42), a command recognition unit (44), an interrupt vector protection unit (50), an address recognition unit (52), a protected FAT (32) and a disk access protection unit (54). These components function together to define a protected FAT (32) implemented on an EEPROM (Electrically Erasable Read-Only Memory). The protected FAT (32) stores the interrupt vectors of executable files, operating system files, and other files commonly attacked by viruses. Before a command is executed, its associated interrupt vectors are compared with the interrupt vectors stored in the protected FAT (32). If the interrupt vectors are the same, the command is executed. Otherwise, there could be an alteration of the executable file, and the command is not executed.

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.

AT	Austria	FR	France	MR	Mauritania
AU	Australia	GA	Gabon	MW	Malawi
BB	Barbados	GB	United Kingdom	NL	Netherlands
BE	Belgium	GN	Guinea	NO	Norway
BF	Burkina Faso	GR	Greece	NZ	New Zealand
BG	Bulgaria	HU	Hungary	PL	Poland
BJ	Benin	IE	Ireland	PT	Portugal
BR	Brazil	IT	Italy	RO	Romania
CA	Canada	JP	Japan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo	KR	Republic of Korea	SE	Sweden
CH	Switzerland	KZ	Kazakhstan	SK	Slovak Republic
CI	Côte d'Ivoire	LJ	Liechtenstein	SN	Senegal
CM	Cameroon	LK	Sri Lanka	SU	Soviet Union
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	MC	Monaco	TG	Togo
DE	Germany	MG	Madagascar	UA	Ukraine
DK	Denmark	ML	Mali	US	United States of America
ES	Spain	MN	Mongolia	VN	Viet Nam
FI	Finland				

COMPUTER PROTECTION DEVICE

FIELD OF THE INVENTION

The present invention relates generally to hardware and software for protecting data stored on a computer.

BACKGROUND OF THE INVENTION

Computer viruses are computer programs which, without the knowledge of a user, enter a computer and execute. These programs often wreak havoc with the proper operation of the computer and can also alter stored data.

A computer virus program enters a computer as an unknown add-on to an executable program. When the user executes the desired executable program, the virus program is also executed, without the knowledge of the user. During execution of the desired executable program, the virus program typically ensures that it will be executed again, whether or not the user again executes the desired executable program. It does this, for example, by copying itself into a new executable file and/or becoming a Terminate and Stay Resident (TSR) program, a program which is always available.

Another method in which the virus ensures it will be executed again is by redefining the interrupt vector of the computer. The interrupt vector is a coded list of addresses to be referenced whenever an interrupt code is received. Some typical interrupt codes relate to the pressing of a key on the keyboard and the movement of a mouse. The addresses in the interrupt vector are the first addresses in memory where operations to be executed upon receipt of the appropriate code are stored.

A virus might alter or "redefine" the addresses of the interrupt vector such that the new addresses stored point to addresses in memory where the virus has stored its own operations to be executed when an interrupt code is received. Typically, the virus operations include the operation the user expects to see as well as other, undesired operations. Thus, for example, if the

user causes a keypress interrupt, the typed key will be displayed, as normally occurs, and, in addition, the operations of the virus will be performed.

Anti-virus programs are well known in the art. They are developed by analyzing the operation of a particular virus program or family of virus programs, much as an anti-viral drug is produced once the operating mode of a human virus or group of viruses is understood. Thus, for each known virus program or group of programs, there is an anti-virus program.

Some anti-virus programs just identify that a virus exists on a user's machine. Others remove the virus upon discovering it.

One method of identifying a virus is to check for any strange operational behavior, such as unexplained changes in the size of files, in the format of data, or in the interrupt vector. Another method is by identifying that there is a known string of bytes known to be a virus.

Most anti-virus programs do not work against new and unknown virus programs or groups of programs. One anti-virus program which appears to protect against unknown virus programs is the Anti-Virus Program manufactured by Iris Software and Computers of Givatayim, Israel. The Anti-Virus Program appears not to allow virus programs to install themselves on a hard disk of a computer and it does this by continuously checking the memory of the computer during operation.

In addition to protection against undesired virus programs, computer users often need to protect their files from undesired access by other users of the computer. For example, some files, such as system-wide files, should never be altered, except by certain authorized personnel. These files need protection against reading, writing or copying.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a system and method for discovering the execution of a computer virus program and for protection data stored in a computer from attack or damage. The present invention operates without any knowledge of the characteristics of any virus programs.

It is a further object of the present invention not to expose protected data to an unauthorized user.

There is therefore provided, in accordance with an embodiment of the present invention, apparatus for protecting access to at least one selected area of a disk. The apparatus includes apparatus for defining the selected area of the disk, apparatus for determining that a disk access command has issued for at least a portion of the selected area and apparatus for disabling the disk access command.

There is further provided, in accordance with an embodiment of the present invention, apparatus for protecting data stored on a disk of a computer. The apparatus includes apparatus for determining when the computer issues one of a predetermined set of commands and apparatus, responsive to the issued command, for selectively interfering with the normal operation of the computer.

There is still further provided, in accordance with an embodiment of the present invention, apparatus for protecting the operation of a computer having active memory. The apparatus includes apparatus for defining that at least one executable file is clean, apparatus for determining when the computer is commanded to load a first executable file into the active memory, apparatus for storing an interrupt vector from a previously loaded executable file if the first executable file is not clean and for enabling the first executable file to load and to execute and apparatus for restoring the stored interrupt vector once the first executable file finishes executing.

Additionally, in accordance with an embodiment of the present invention, the disk access command is a selected one of a

write, read or format command. The predetermined set of commands includes write, read, format and load commands.

Furthermore, in accordance with an embodiment of the present invention, the apparatus includes apparatus for identifying a user and a classification level of the user. The apparatus also includes apparatus for classifying access levels for data stored in the at least one selected area.

Still further, in accordance with an embodiment of the present invention, the apparatus for disabling includes apparatus for authorizing performance of the disk access command if the apparatus for identifying a user indicates that the user has a classification level equivalent to or larger than the access level for data to be accessed.

Moreover, in accordance with an embodiment of the present invention, the apparatus includes apparatus for defining accompanying files to be opened when the first executable file is loaded and apparatus for closing the accompanying files if another executable file is commanded to be loaded.

Additionally, in accordance with an embodiment of the present invention, the disk forms part of a computer and the apparatus for disabling or the apparatus for selectively interfering include a stop and hold command to the computer. Alternatively, the apparatus for disabling or the apparatus for selectively interfering include a non-maskable interrupt to the computer. A further alternative for the apparatus for disabling or the apparatus for selectively interfering is an analog switch.

There is further provided, in accordance with an embodiment of the present invention, apparatus for protecting at least one selected area of a disk of a computer from undesired access operations, the computer including a disk controller and a bus. The apparatus includes apparatus connected in parallel to the bus for determining that an undesired access command to a portion of the selected area of the disk has issued and apparatus for disabling the undesired access command.

There is still further provided, in accordance with an embodiment of the present invention, a computer network including

a multiplicity of computer workstations each usable by one user at one time and each having a workstation storage medium, a file server for storing files accessible by each of the computer workstations, the file server having a server storage medium, workstation protection apparatus for protecting access to at least one selected area of the workstation storage medium and server protection apparatus for protecting access to at least one selected area of the server storage medium. The server protection apparatus communicates with each of the workstation protection apparatus to provide information regarding the selected area of the server storage medium.

Additionally, in accordance with the network embodiment of the present invention, the server protection apparatus and the workstation protection apparatus include apparatus for defining the at least one selected areas of the storage media, apparatus for determining that a disk access command has issued for at least a portion of the selected areas and apparatus for disabling the disk access command.

Furthermore, in accordance with the network embodiment of the present invention, the server protection apparatus and the workstation protection apparatus include apparatus for determining when the computer issues one of a predetermined set of commands and apparatus, responsive to the issued command, for selectively interfering with the normal operation of the computer.

Finally, in accordance with the network embodiment of the present invention, the workstations and the file server have active memories. The server protection apparatus and the workstation protection apparatus include apparatus for defining that at least one executable file is clean, apparatus for determining when the computer is commanded to load a first executable file into the active memory of one of the workstations, apparatus for storing an interrupt vector from a previously loaded executable file if the first executable file is not clean and for enabling the first executable file to load and to execute and apparatus for restoring the stored interrupt vector once the first executable file finishes executing.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a general block diagram illustration of interaction of apparatus for data protection constructed and operative in accordance with the present invention with a computer;

Fig. 2 is a block diagram illustration of the elements of the apparatus for protection of Fig. 1;

Fig. 3 is a more detailed block diagram illustration of the interaction shown in Fig. 1;

Fig. 4 is a flow chart illustration of the overall operations of the apparatus of the present invention;

Fig. 5 is a flow chart illustration of the operation of identifying a load command, useful in the operations of Fig. 4;

Fig. 6 is a flow chart illustration of the operation of identifying the file name, useful in the operations of Fig. 4;

Fig. 7 is a flow chart illustration of the operation of saving an interrupt vector, useful in the operations of Fig. 4;

Fig. 8 is a flow chart illustration of the operation of restoring an interrupt vector, useful in the operations of Fig. 4;

Fig. 9 is a flow chart illustration of changing parameters of operation of the apparatus of Fig. 1, useful in the operations of Fig. 4;

Fig. 10 is a flow chart illustration of the operations of disabling the operation of the computer, useful in the operations of Fig. 4;

Fig. 11 is a flow chart illustration of installation operations, useful in the operations of Fig. 4; and

Fig. 12 is a block diagram illustration of a plurality of the apparatus of Fig. 2 connected together in a network.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Reference is now made to Fig. 1 which illustrates, in block diagram format, the operation of a protection device 10 of the present invention when operating to protect a computer 12 against the operation of a virus. The computer 12 is typically a personal computer and comprises a Central Processing Unit (CPU) 14 having a low frequency clock 15, such as an 80286 CPU manufactured by Intel of the U.S.A. with a 6 MHz clock, a Random Access Memory (RAM) 16, a disk 18 and a disk controller 20, such as the 82064 controller also manufactured by Intel. The disk 18 can be a hard disk or a floppy disk.

Typically, the elements of the personal computer come in a housing which is large enough to hold other elements, such as a modem.

Computer 12 typically operates under an operating system, such as the Disk Operating System (DOS) 22 of Microsoft Inc. of the USA. DOS stores information regarding each file on the disk 18 in a File Allocation Table (FAT) 24. The FAT 24 typically includes a list, per file, of the portions of the disk 18, known as sectors, which are allocated to each file.

The protection device 10 is typically located within the housing of the computer 12 and typically communicates with the computer 12 via a bus 26 of computer 12. Bus 26 can be any suitable bus, such as the Industrial Standard Architecture (ISA) AT bus.

Protection device 10 is operative to protect the computer 12 from unauthorized memory access, such as accessing the disk 18, and from the effects of redefinition of the interrupt vector.

To protect unauthorized memory access, the user defines, through protection device 10, a protected area 30 on disk 18. The protection device 10 stores within itself a listing of the locations, or sectors, of the disk 18 which are within protected area 30. This listing is known as the protected area FAT 32.

Typically, the user will store within the protected area 30 those files most important to him, such as those relating to his operating system, his most commonly used executable files and any data which he desires not to be damaged. Furthermore, the user will place in the protected area 30 only those files which he knows are clean, or have no viruses attached to them.

If the protection device 10 detects a disk access command, either a write, read or format disk command, which addresses a section of the protected area 30, protection device 10 will only enable the disk access if an authorized user authorizes it.

Furthermore, the protection device 10 monitors the commands of the CPU 14 for a load command in which an executable file, such as a program or a virus, is loaded into RAM 16.

If the loaded file is not known to be clean from viruses, there is a possibility that the viruses, if any, will redefine the interrupt vector. Therefore, the interrupt vector of the previously loaded file, assuming it was a file known to be clean, is saved before loading the new executable file. When the present executable file finishes executing, the protection device 10 retrieves the saved interrupt vector. In this manner, the changed interrupt vector will be active only as long as the present executable file is executing.

If desired, data files which are typically opened when a given executable file is executing, can be indicated as such. These "accompanying data files" are then opened upon loading of the executable file and are closed when the executable files ceases operating. Specifically, if an executable file is commanded to be loaded while the accompanying data files of a previously loaded executable file are still open, the protection unit 10 closes the accompanying data files before allowing the newly commanded executable file to load.

Reference is now made to Fig. 2 which illustrates, in block diagram format, the elements of the protection device 10. Protection device 10 typically comprises a manager 40 for managing the operations of protection device 10, a protected area definition unit 42 for defining protected area 30 and for identi-

fyng the files which are to be placed in protected area 30, and a command recognition unit 44 for recognizing when one of a predetermined set of commands is produced by the computer 12.

The manager 40 provides installation operations, and classification and identification of system users.

If desired, users can be classified by the level of access to the protected files in the protected area 30 permitted them. For instance, it may be desired to define two access levels, one of "system operator" and one of a "regular operator". The system operator is allowed to access system files, such as files pertaining to the operating system, and application files. The regular operator is allowed to access only application files.

For this purpose, users are provided with user names and external means for identification 46, such as passwords, special codes or magnetic cards, such as credit cards.

The means for identification 46 are provided to an identification unit 48, such as a keyboard of computer 12 for receiving passwords and such as a magnetic card reader, such as those produced by Neuron Corporation of Tokyo, Japan, for receiving magnetic cards. The identification unit 48 compares the identification received to that expected for the specific user and notifies the manager 40 whether or not there is a match. Without a match, the user cannot access the files in the protected area 30. With a match, the user can access the files permitted for his access level.

If the identification unit 48 indicates that the user is authorized, then protected area definition unit 42 enables the selected files to be defined as protected. The definition operation is performed as follows:

The protected area definition unit 42 requires that CPU 14 provide it with a copy of FAT 24. Unit 42 then searches FAT 24 for the sector or sectors on disk 18 in which the selected files are stored. These addresses are then stored in protected FAT 32 which, in turn, is stored in an Electronically Erasable Programmable Read Only Memory (EEPROM) 68, shown in Fig. 3 and described in more detail hereinbelow.

The protected area definition unit 42 enables the user to define which files are to be protected and to provide classification levels for them. For the example hereinabove, the system files will have a level of "system operator only" and the application files will have a level of "everyone allowed".

Unit 42 also enables the user to indicate which executable files are known to be clean, or free of viruses.

Thus, the protected FAT 32 also contains classification level information and cleanliness status information for each file protected.

Since viruses typically attack executable files and operating system files, the user will typically select protection for the entirety of his executable files as well as his operating system files, partition table and boot sector. Protection can also be placed on data which the user does not want to be altered or read.

The command recognition unit 44 monitors bus 26 for commands, comparing every received command with the predetermined set of commands. The predetermined set typically comprises any read, write or loading commands. These also include formatting commands which effectively rewrite the entire disk 18.

If a received command is one of the set, the command recognition unit 44 determines if it is a load command. If so, unit 44 provides control to an interrupt vector protection unit 50. If not, indicating that a disk access operation is about to take place, unit 44 provides control to an address recognition unit 52.

Address recognition unit 52 compares the address associated with the command to the sector addresses stored in the protected FAT 32 and checks the classification level for the addressed sector. If there is a match, indicating that the computer 12 is attempting to access protected area 30, unit 52 issues a stop command to a disk access protection unit 54 to disable the access attempt. Unit 52 then requests that the user provide authorization for the access of area 30. The user then has to provide its identification means 46 to identification unit

48.

If the user is authorized to access the file, then the disk access is enabled and control is returned to command recognition unit 44.

If the user cannot provide authorization or if a virus tried accessing the protected area 30, no action is taken. The user is thus notified as soon as a virus program attempts to write to the disk or an unauthorized user tries to access the area 30. If the user wishes to reenable disk access, he typically has to restart, or "reboot" the computer 12.

The command recognition unit 44 identifies a load command by identifying that a command to write to a predetermined address in RAM 16 has been issued. The predetermined address is the address into which the first address of the executable file to be loaded is stored.

The interrupt vector protection unit 50 first disables access to any accompanying data files of the previously loaded executable file, herein called the "first" executable file. Unit 50 then identifies the executable file about to be loaded, henceforth called the "second" executable file, by comparing the addresses of the second executable file with those stored in the protected FAT 32.

If the second executable file is clean according to the protected FAT 32, access to its accompanying files is enabled, by placing the accompanying files into the protected FAT 32, and control is returned to the command recognition unit 44.

If the second executable file is not clean, indicating that it contains either a virus or a program which the user is not protecting, then unit 50 stops the operation of CPU 14, reads the current interrupt vector which belongs to the previous executable file and stores the interrupt vector in EEPROM 68 (Fig. 3). The CPU 14 is then released and control of the protection unit 10 is returned to the command recognition unit 44 and the second executable file is allowed to execute.

When a new executable file, herein called the "third" executable file, is loaded after a second executable file which

was not clean, the interrupt vector protection unit 50 replaces the interrupt vector of the second executable file, which may have been defined to address undesirable operations, with the interrupt vector of the first executable file.

The replacement operation includes the steps of stopping CPU 14, writing the stored interrupt vector into the interrupt vector storage addresses in RAM 16, and releasing CPU 14.

After replacing the interrupt vector, unit 50 checks that the third executable file is clean. If not, then unit 50 saves the interrupt vector, which is now that of the first executable file. Unit 50 then proceeds as described hereinabove.

Reference is now made to Fig. 3 which illustrates, in block diagram format, the hardware elements of the present invention.

Protection device 10 typically comprises a microprocessor 60 with a high frequency clock 62, such as the 80386DX microprocessor manufactured by Intel of the USA with a 33 MHz clock, working in conjunction with a RAM 64. Microprocessor 60 typically is associated with at least one input/output port 66 which is connected to bus 26.

Microprocessor 60 is further associated with Electronically Erasable Programmable Read Only Memory (EEPROM) 68 for storing the predetermined set of commands, protected FAT 32, interrupt vectors, passwords and user names.

Microprocessor 60, in conjunction with RAM 64, typically implements the manager 40, the protected area definition unit 42, the command recognition unit 44, the interrupt vector protection unit 50 and the address recognition unit 52.

The disk access protection unit 54 can be embodied in a number of ways. Unit 54 can be embodied as a hold and a stop command. The hold command is transmitted, via bus 26, to the CPU 14 which causes the CPU 14 to stop its operation. At the same time, the stop command is sent, also via bus 26, to disk controller 20 to stop its operation. This embodiment is operative for those disk controllers, such as the 82064 mentioned hereinabove, which can respond to a stop command.

Alternatively, unit 54 can be embodied as an analog switch, such as the SN74ALS1244 manufactured by Texas Instruments of U.S.A., or as a mechanical relay. The switch or relay is connected to the power cable (not shown) of disk 18 and, when activated, disconnects the power to disk 18.

For a bus 26 which has a non-maskable interrupt, such as a microchannel bus or an Enhanced ISA (EISA) bus, unit 54 can be embodied as a non-maskable interrupt which is sent directly to CPU 14. The interrupt causes the CPU 14 to execute a routine stored therein which cancels the access command and/or reboots the system.

Optionally, microprocessor 60 can provide a notice to CPU 14 that will indicate, upon rebooting, that the cause of the stopping of the computer 12 was a virus or unauthorized access, and not something else.

It will be appreciated that unit 54 can include a combination of the above-described disabling methods and mechanisms.

It will be appreciated that the combined operations of command recognition unit 44, address recognition unit 52 and disk access protection unit 54 are fast enough to finish performing in one clock cycle of computer 12.

It will further be appreciated that the protection device 10 of the present invention ensures that a virus which tries to access protected area 30 generally will have no effect. The protection device 10 discovers the virus as soon as it attempts to access the data in the protected area 30, thereby indicating to the user which file or program is affected by the virus. Additionally, any changes to the interrupt vector created by the virus are effective only during the operating time of the virus.

The present invention is advantageous in that the device 10 is a hardware device that operates in parallel to computer 12 and is not operated by computer 12, thus making it difficult for a virus to overcome the operation of the device. Furthermore, the device 10 operates generally without any knowl-

edge of the characteristics of virus programs.

It will also be appreciated that the protection device 10 does not add a significant amount of time to the operation of computer 12 since the microprocessor 60 operates in parallel to bus 26. The method of identifying unauthorized access, described hereinabove, can be applied to any suitable computer.

Reference is now made to Figs. 4 - 11 which together illustrate the operations of the protection device 10. The operations of Figs. 4 - 11 are typically performed in software stored in the EEPROM 68 of protection device 10. The figures are believed to be self-explanatory and therefore, in the interest of conciseness, they will not be described in great detail.

In general terms, the figures describe the following:

Fig. 4 describes the overall operations of the protection device 10;

Fig. 5 describes the operation of identifying a load command;

Fig. 6 describes the operation of identifying the name of a loaded executable file;

Fig. 7 describes the operation of saving an interrupt vector;

Fig. 8 describes the operation of restoring an interrupt vector;

Fig. 9 describes an update program for changing parameters of operation of the protection device 10, where typical parameters are the files which are in the protected area 30, the access levels of users, the classification levels of the protected files, and the clean status of each file;

Fig. 10 describes the operations of disabling the operation of the computer; and

Fig. 11 describes installation operations.

It will be noted that the update program illustrated in Fig. 9 is typically performed by software stored in the protected area 30 and loaded into RAM 16. The interface between the user and the software is through computer 12.

Furthermore, the program of Fig. 9 enables and disables

access to accompanying files. Enabling is performed by modifying the protected FAT 32 to include the accompanying files. Disabling is performed by modifying the protected FAT 32 to no longer include the accompanying files.

The installation program whose operations are illustrated in Fig. 11 serves to identify the type of CPU 14, the peripheral apparatus attached to computer 12 and the version of the operating system under which everything operates. Furthermore, the program calls the software uses the update program of Fig. 9 in order to define the parameters of operation.

It is desired to execute the installation program, from an external disk, after a low level format and after installing the operating system.

Reference is now made to Fig. 12 which illustrates a plurality of computers connected together via a network 100. Typically, in network operations, there are a multiplicity of workstations 102 which save their files onto a file server 104.

In accordance with the present invention, protection devices are installed in each of workstations 102 and the file server 104. In Fig. 12, the protection devices on workstations 102 are labeled 106 and the protection device on the file server is labeled 108.

The protection devices 106 and 108 operate generally as described hereinabove with the following exceptions:

The protection device 108 maintains a network-wide protected FAT 32 describing the status of the files stored on the file server 104. Whenever one of the workstations 102 is started or "booted", its protection device 106 checks the date on the protected FAT 32 of protection device 108. If the date is later than the date on the protected FAT 32 of the protection device 106 of the workstation 102, the protection device 106 receives from protection device 108 a copy of its protected FAT 32.

Furthermore, whenever a user of one of the workstations 102 desires to change its protected FAT 32, and thus, the network-wide FAT 32, the new, updated version of FAT 32 is broadcast

to the remaining workstations 102.

It will be appreciated that the protection devices 106 and 108 additionally comprise time clocks (not shown) which operate independently of the time clocks of the workstations. The protection devices 106 monitor the time clocks of the workstations 102 to ensure that the workstation time matches the protection device time and to update the workstation time if it does not match the protection device time. Similarly, the protection device 108 monitors the time of the file server 104.

It will be appreciated by persons skilled in the art that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention is defined only by the claims that follow:

CLAIMS

1. Apparatus for protecting access to at least one selected area of a disk, the apparatus comprising:
 - means for defining said at least one selected area of said disk;
 - means for determining that a disk access command has issued for at least a portion of said at least one selected area; and
 - means for disabling said disk access command.

2. Apparatus for protecting data stored on a disk of a computer, the apparatus comprising:
 - means for determining when said computer issues one of a predetermined set of commands; and
 - means, responsive to said issued command, for selectively interfering with the normal operation of said computer.

3. Apparatus for protecting the operation of a computer having active memory, the apparatus comprising:
 - means for defining that at least one executable file is clean;
 - means for determining when said computer is commanded to load a first executable file into said active memory;
 - means for storing an interrupt vector from a previously loaded executable file if said first executable file is not clean and for enabling said first executable file to load and to execute; and
 - means for restoring said stored interrupt vector once said first executable file finishes executing.

4. Apparatus according to claim 1 and wherein said disk access command is a selected one of a write, read or format command.

5. Apparatus according to claim 2 and wherein said prede-

terminated set of commands includes write, read, format and load commands.

6. Apparatus according to claim 1 and including means for identifying a user and a classification level of said user.

7. Apparatus according to claim 1 and including means for classifying access levels for data stored in said at least one selected area.

8. Apparatus according to claim 6 and wherein said means for disabling include means for authorizing performance of said disk access command if said means for identifying a user indicate that said user has a classification level equivalent to or larger than said access level for data to be accessed.

9. Apparatus according to claim 2 and including means for identifying a user and a classification level of said user.

10. Apparatus according to claim 3 including means for defining accompanying files to be opened when said first executable file is loaded and means for closing said accompanying files if another executable file is commanded to be loaded.

11. Apparatus according to claim 1 wherein said disk forms part of a computer and wherein said means for disabling include a stop and hold command to said computer.

12. Apparatus according to claim 1 wherein said disk forms part of a computer and wherein said means for disabling include a non-maskable interrupt to said computer.

13. Apparatus according to claim 1 and wherein said means for disabling include an analog switch.

14. Apparatus according to claim 2 and wherein said means for selectively interfering include a stop and hold command to said computer.

15. Apparatus according to claim 2 and wherein said means for selectively interfering include a non-maskable interrupt to said computer.

16. Apparatus according to claim 2 and wherein said means for selectively interfering include an analog switch for disabling operation of said disk.

17. Apparatus for protecting at least one selected area of a disk of a computer from undesired access operations, the computer comprising a disk controller and a bus, the apparatus comprising:

means connected in parallel to said bus for determining that an undesired access command to a portion of said at least one selected area of said disk has issued; and

means for disabling said undesired access command.

18. A computer network comprising:

a multiplicity of computer workstations each usable by one user at one time and each having a workstation storage medium;

a file server for storing files accessible by each of said computer workstations, the file server having a server storage medium;

workstation protection means for protecting access to at least one selected area of said workstation storage medium; and

server protection means for protecting access to at least one selected area of said server storage medium,

wherein said server protection means communicates with each of said workstation protection means to provide information

regarding said at least one selected area of said server storage medium.

19. A computer network according to claim 18 and wherein said server protection means and said workstation protection means comprise:

means for defining said at least one selected areas of said storage media;

means for determining that a disk access command has issued for at least a portion of said at least one selected areas; and

means for disabling said disk access command.

20. A computer network according to claim 18 and wherein said server protection means and said workstation protection means comprise:

means for determining when said computer issues one of a predetermined set of commands; and

means, responsive to said issued command, for selectively interfering with the normal operation of said computer.

21. A computer network according to claim 18 wherein said workstations and said file server have active memories and wherein said server protection means and said workstation protection means comprise:

means for defining that at least one executable file is clean;

means for determining when said computer is commanded to load a first executable file into said active memory of one of said workstation;

means for storing an interrupt vector from a previously loaded executable file if said first executable file is not clean and for enabling said first executable file to load and to execute; and

means for restoring said stored interrupt vector once said first executable file finishes executing.

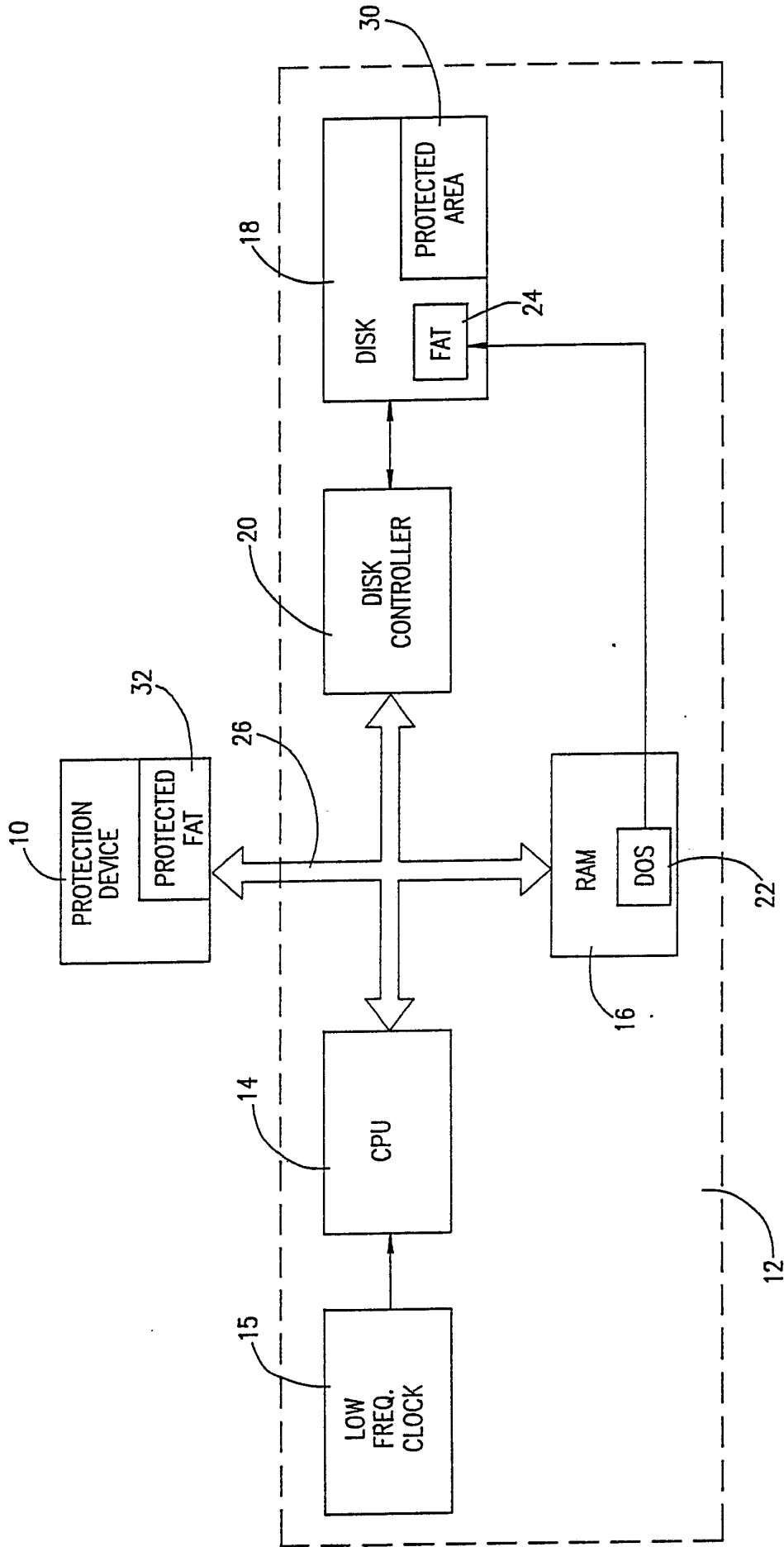
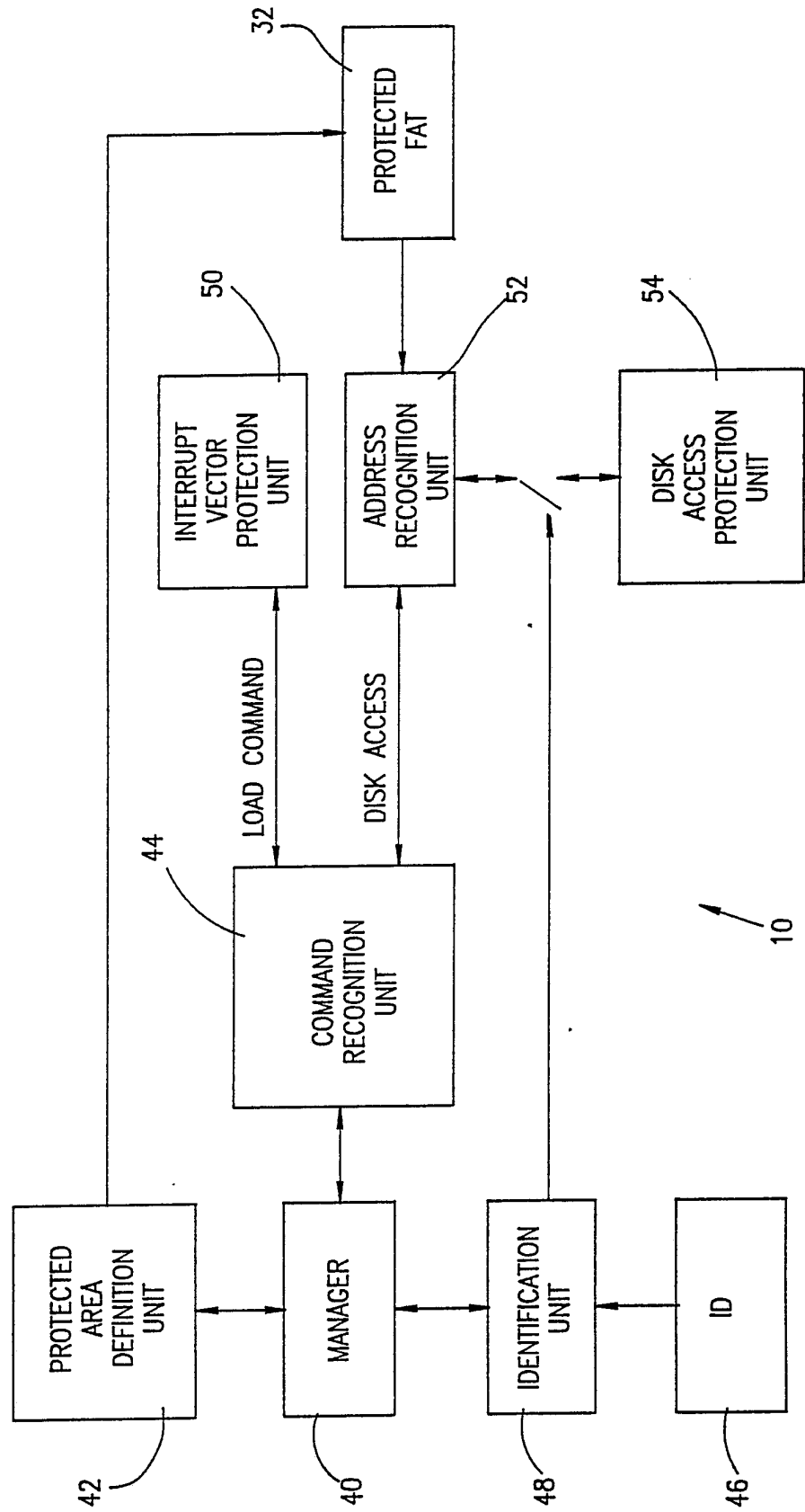


FIG. 1

FIG.2



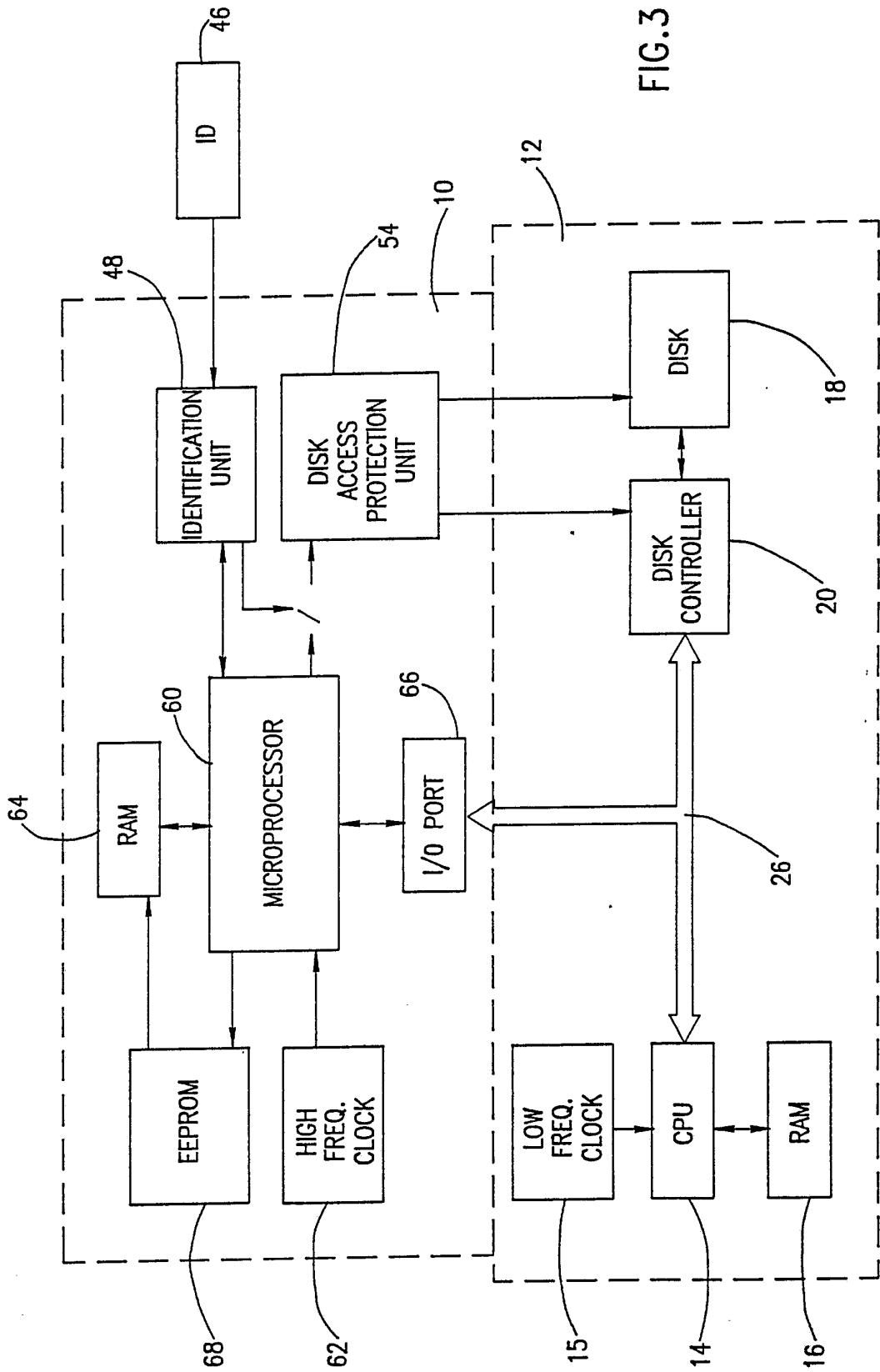


FIG. 3

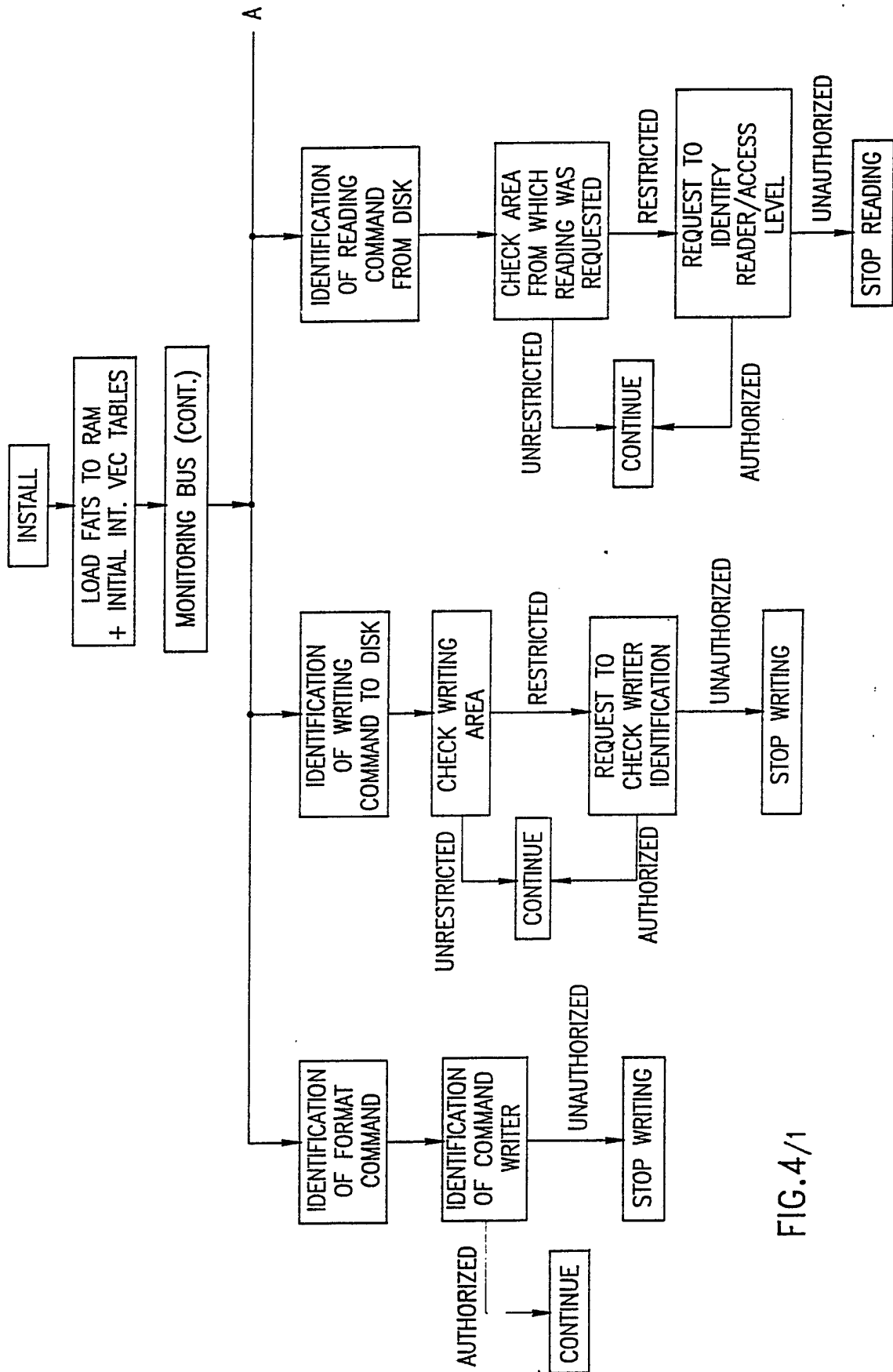


FIG. 4/1

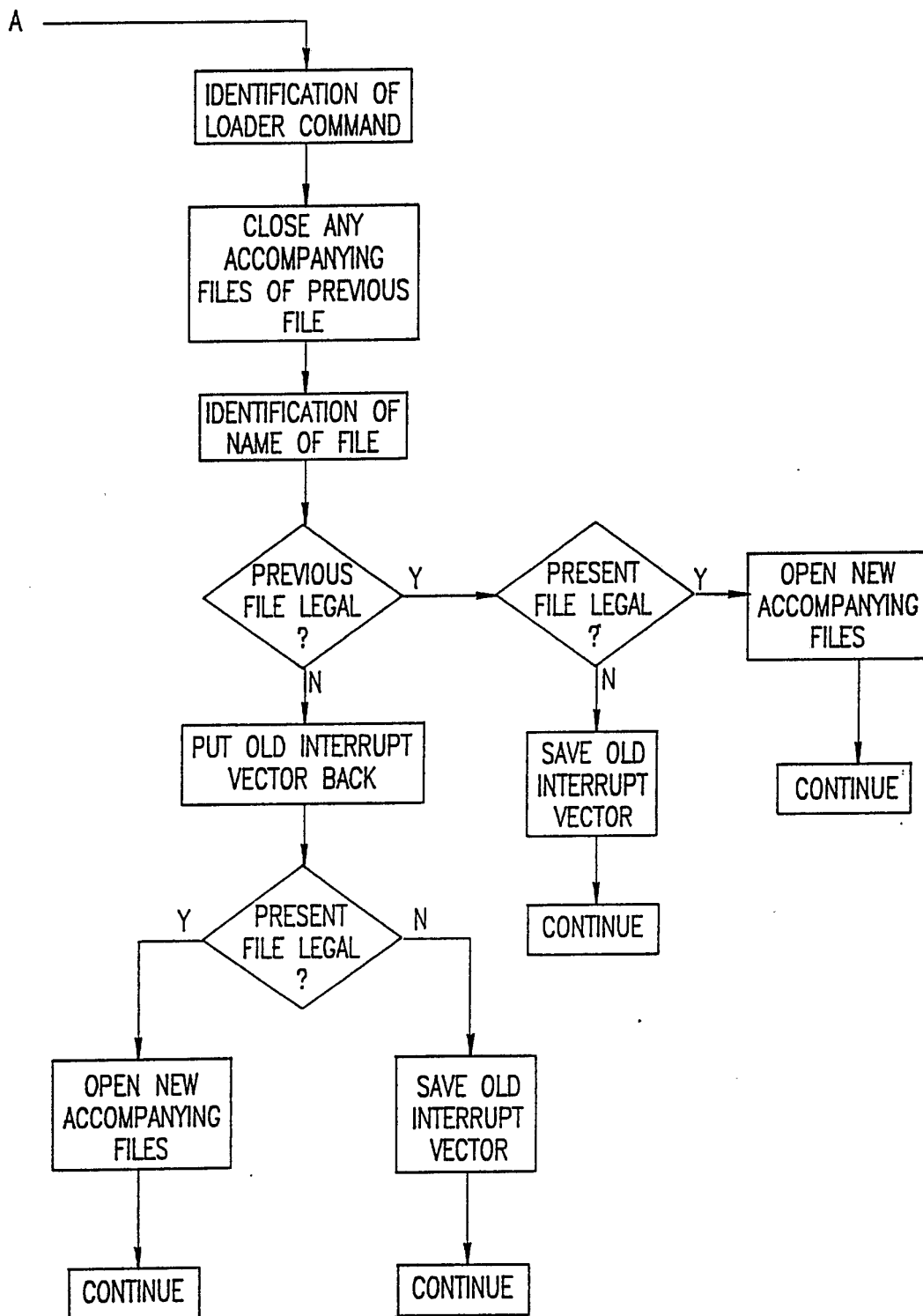


FIG.4/2

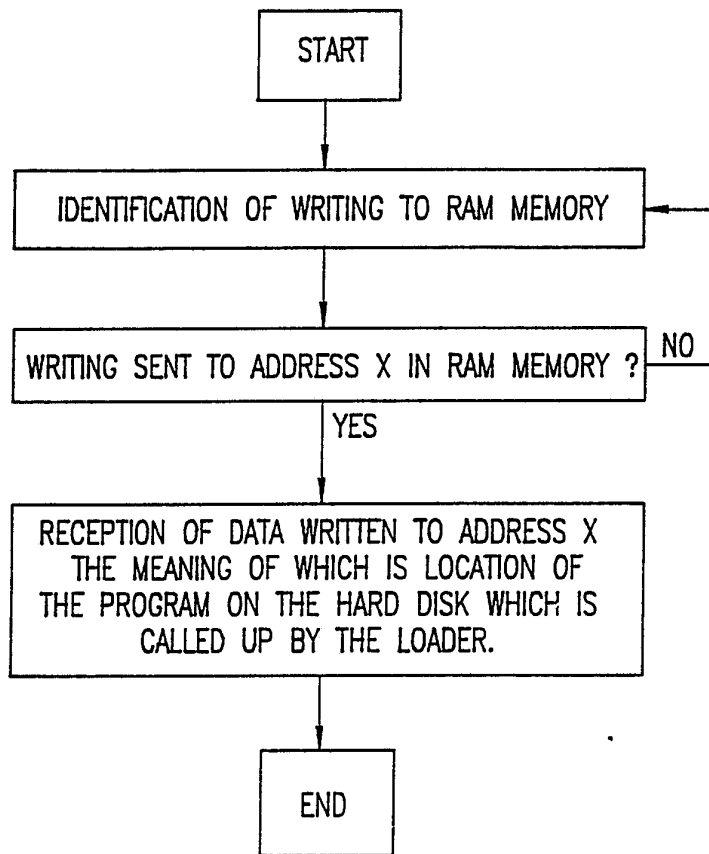


FIG.5

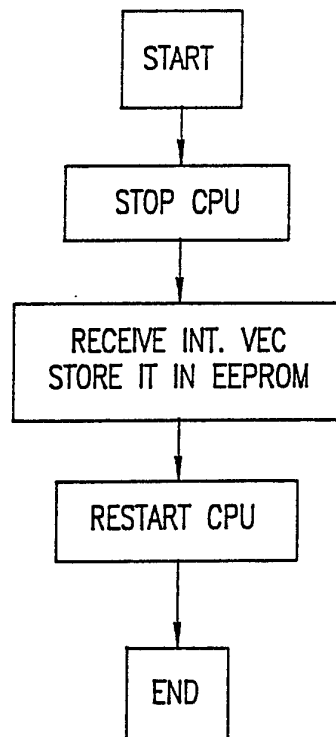


FIG.7

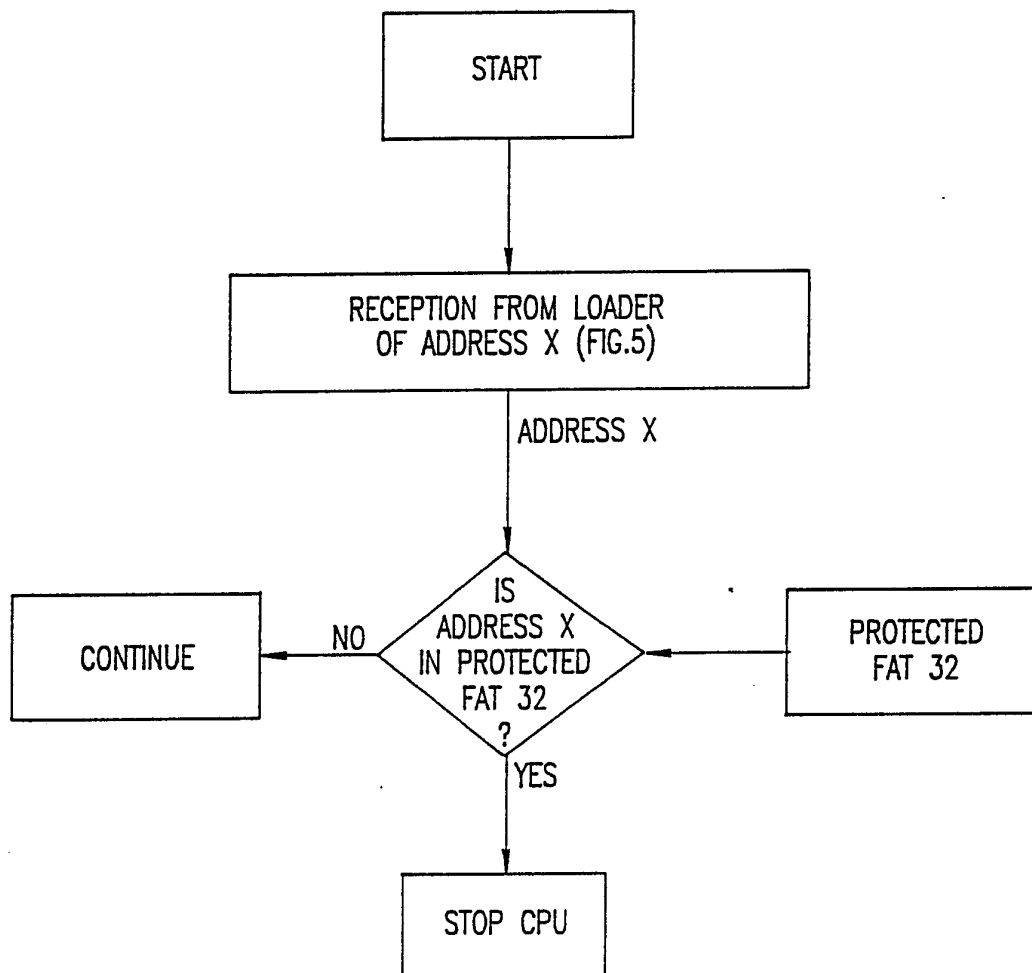


FIG.6

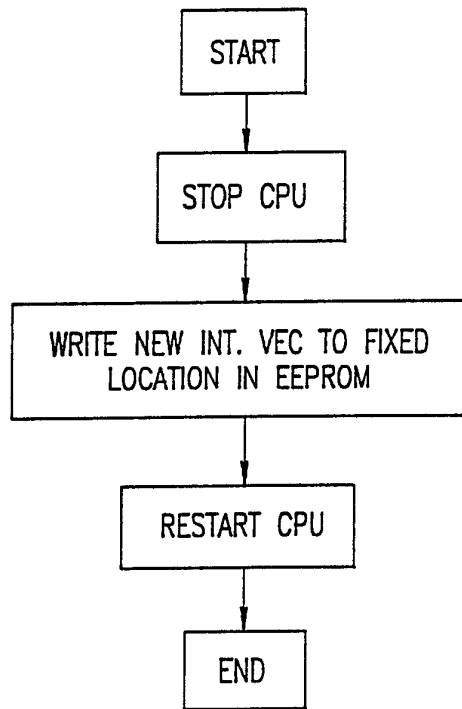


FIG.8

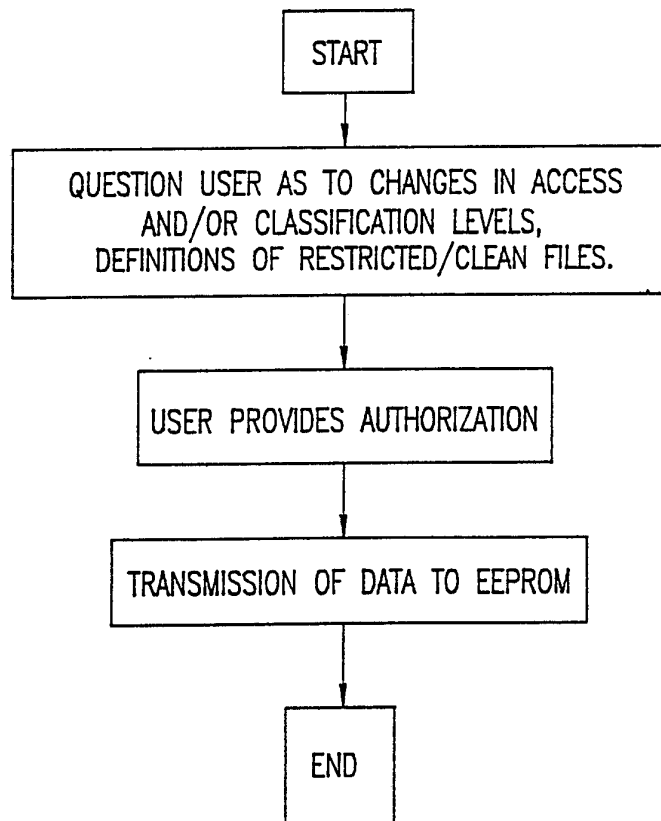


FIG.9

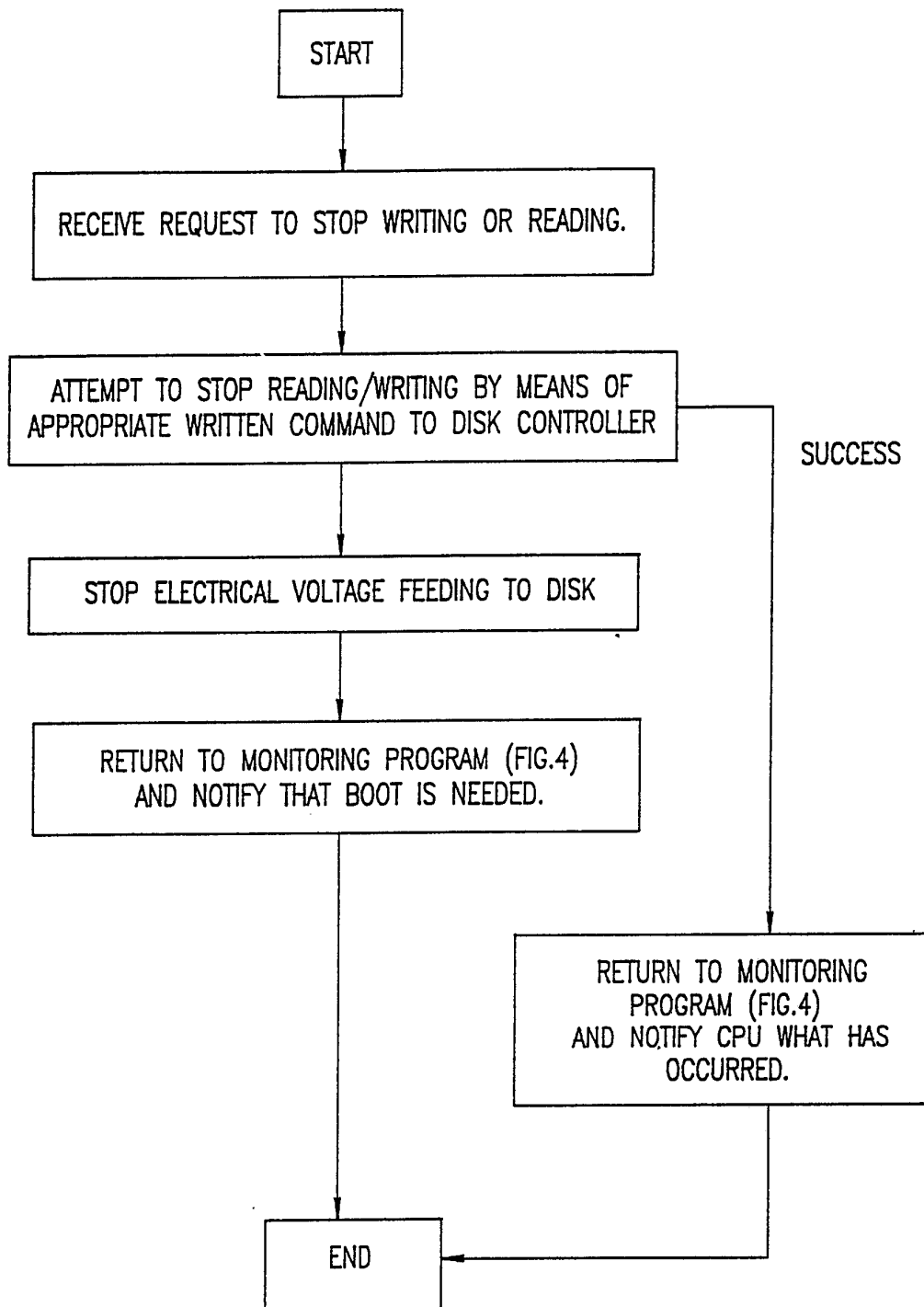


FIG.10

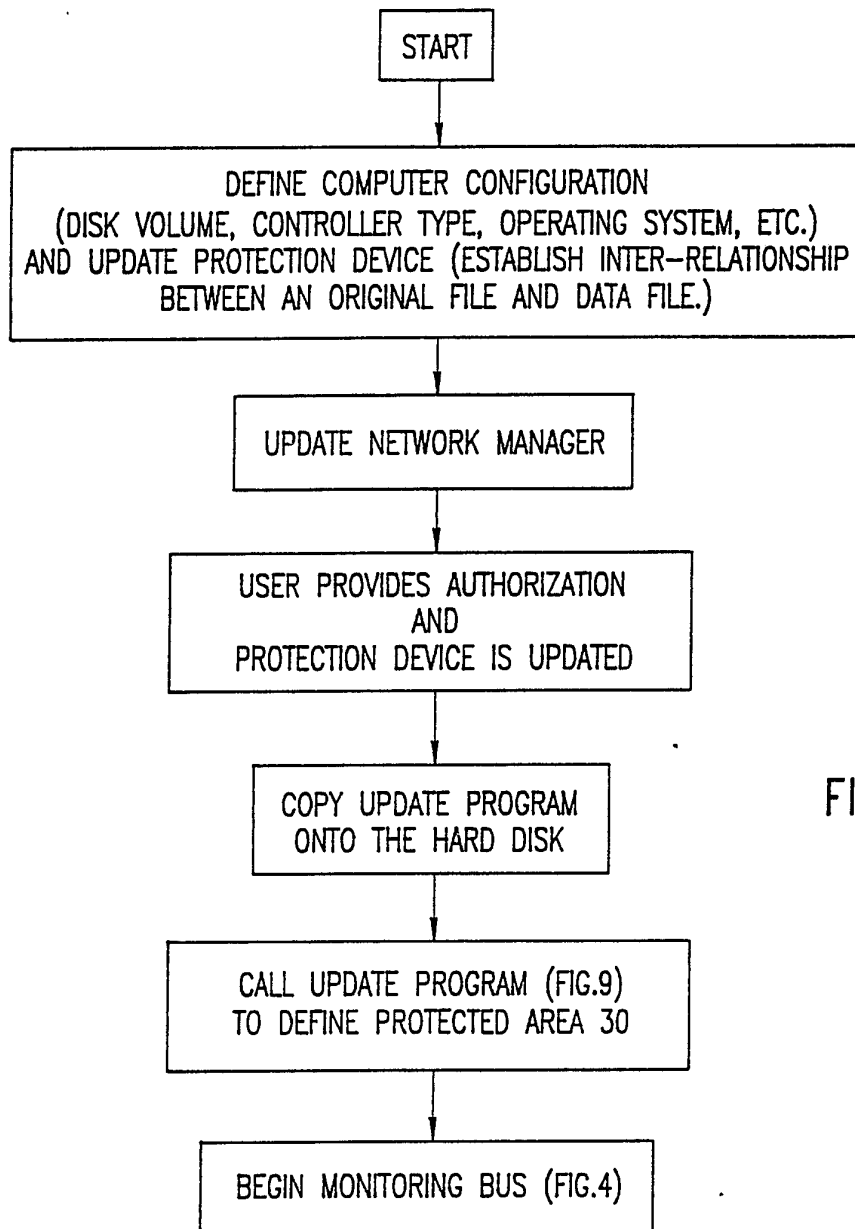


FIG.11

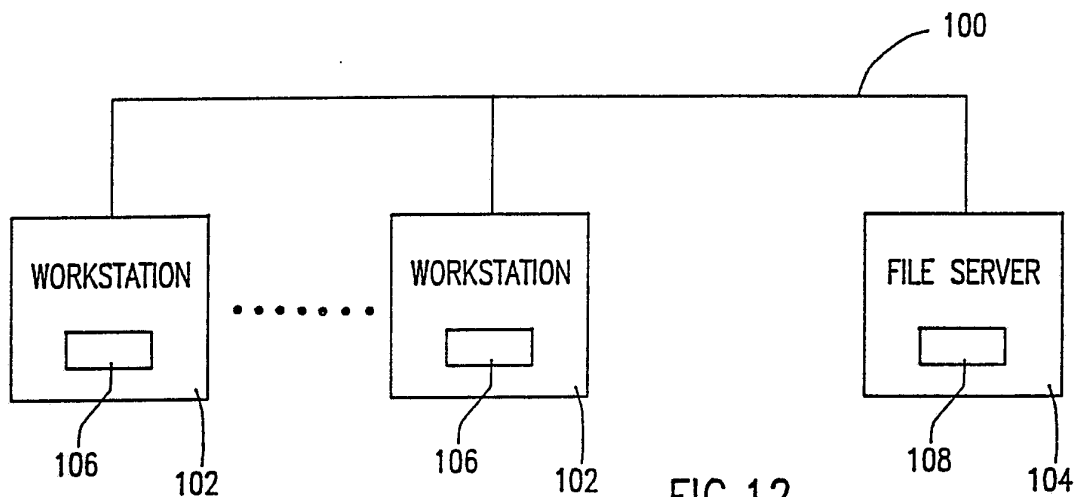
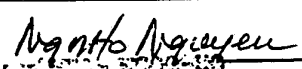


FIG.12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US92/11374

<p>A. CLASSIFICATION OF SUBJECT MATTER IPC(5) :GO6F 9/06 GO6F 15/24 US CL :395/650, 700 According to International Patent Classification (IPC) or to both national classification and IPC</p>																				
<p>B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) U.S. : 364/969, 969.1, 969.2, 969.3, 969.4, 918.7, 364/246.6</p> <p>Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched IEEE/IEE Publications Ondisc</p> <p>Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) USPAT automated patent system security and computer and access and denied and (rom or ceprom).</p>																				
<p>C. DOCUMENTS CONSIDERED TO BE RELEVANT</p> <table border="1"> <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, A, 4,757,533 (Allen et al) 12 July 1988. Column 5, lines 5-40. Column 5, line 25, Column 2, lines 30-40, Column 1, lines 50-54 and column 6, lines 36-38 , Column 2, lines 41-57.</td> <td>13,15,16,17,19 1,2,4,5,10,11,12, 15,20 3,21, 6-9, 18</td> </tr> <tr> <td>X</td> <td>US,A, 5,012,514 (Renton) 30 April 1991. Column 3, lines 10-22.</td> <td>1-17,19-21</td> </tr> </tbody> </table>			Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.	X	US, A, 4,757,533 (Allen et al) 12 July 1988. Column 5, lines 5-40. Column 5, line 25, Column 2, lines 30-40, Column 1, lines 50-54 and column 6, lines 36-38 , Column 2, lines 41-57.	13,15,16,17,19 1,2,4,5,10,11,12, 15,20 3,21, 6-9, 18	X	US,A, 5,012,514 (Renton) 30 April 1991. Column 3, lines 10-22.	1-17,19-21									
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.																		
X	US, A, 4,757,533 (Allen et al) 12 July 1988. Column 5, lines 5-40. Column 5, line 25, Column 2, lines 30-40, Column 1, lines 50-54 and column 6, lines 36-38 , Column 2, lines 41-57.	13,15,16,17,19 1,2,4,5,10,11,12, 15,20 3,21, 6-9, 18																		
X	US,A, 5,012,514 (Renton) 30 April 1991. Column 3, lines 10-22.	1-17,19-21																		
<p><input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.</p>																				
<table border="0"> <tr> <td>* Special categories of cited documents:</td> <td>"T"</td> <td>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</td> </tr> <tr> <td>"A" document defining the general state of the art which is not considered to be part of particular relevance</td> <td>"X"</td> <td>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</td> </tr> <tr> <td>"E" earlier document published on or after the international filing date</td> <td>"Y"</td> <td>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</td> </tr> <tr> <td>"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)</td> <td>"&"</td> <td>document member of the same patent family</td> </tr> <tr> <td>"O" document referring to an oral disclosure, use, exhibition or other means</td> <td></td> <td></td> </tr> <tr> <td>"P" document published prior to the international filing date but later than the priority date claimed</td> <td></td> <td></td> </tr> </table>			* 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 part 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		
* 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 part 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 12 FEBRUARY 1993		Date of mailing of the international search report 10 MAR 1993																		
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. NOT APPLICABLE		Authorized officer  MICHAEL T. RICHEY INTERNATIONAL PATENT DIVISION Telephone No. (703) 305-9669																		