REPLACED SHEETS SG
☑ Description : paged 1 to paged 9
☑ Claim(s) : paged 10 to paged 11
☐ Drawing(s) : paged ..... to paged .....
☑ Abstract : paged 12 to paged 12
DATE OF RECEIPT .....

UK9-89-040

IPOS copy
9600140-9

COMPUTER SYSTEM SECURITY DEVICE

The present invention relates to a computer system having multiple levels of security access, and in particular to those computer systems having a power-on password.

IBM Technical Disclosure Bulletin Volume 30 No. 5 October 1987 at pages 57 and 58 discloses a security system for a personal computer. Personal computers such as, for example, the IBM Personal System/2 (IBM and Personal System/2 are trademarks of International Business Machines Corporation) range of computers are provided with a power-on password facility to prevent use of the computer by unauthorised persons; in this case an unauthorised person is a person not knowing the power-on password. In the IBM Personal System/2 range of computers the power-on password is held non-volatile (battery powered) CMOS Random-Access Memory ("RAM").

The power-on password facility provided on the IBM Personal System/2 personal computers is limited to a single password, and once a person has access to that password the full facilities of the computer are available to that person.

It would be desirable to provide access to the computer for a plurality of users and also provide different levels of access to the facilities of the computer. In particular it is desirable to have a computer system in which the way the system boots up after power-on or system reset has been predetermined at the stage of set up and configuration of the system by a system manager or similar such control person. The term "boot" refers to initial program load into the computer memory. In the case of computer systems which are capable of booting from multiple devices (ie from diskette, fixed disk or the like), when the system is switched on initially, a boot (sometimes referred to as bootstrap) program is initialised to load the operating system from a reserved area on the media (this may be on the floppy diskette, fixed disk or remote device) and load the

This Sheet Has Been Replaced

This Sheet Has Been Replaced

operating system. The boot routine is held in the system's Read Only Memory ("ROM") and it is automatically entered after switching on the system or is activated upon acceptance of the user entered power-on password.

In prior art computer systems, password access to the system facilities is activated after the operating system has been loaded. Unauthorised access is possible before the operating system has been loaded by using an alternative boot up program. Once the unauthorised user has succeeded in booting up the system all facilities of the system are vulnerable to misuse.

In order to illustrate the problem of the prior art one may consider the precautions being taken by computer system managers to prevent contamination by computer viruses and the like. A personal computer is conventionally restricted to a single user by a conventional physical key lock or a power-on/configuration password as described above. Any user having such access has unrestricted access and may use the diskette drive if fitted. The most common source of computer viruses is from a diskette contaminated with the virus, either deliberatly or as a result of inadequate screening of stored programs and data on diskette made available to the user. Prior art multi-access computer systems are configured to attempt to boot up from the diskette drive (provided a suitable diskette is inserted) or, if not possible from diskette, to attempt boot up from other storage media eg the fixed disk or remote device. It is clear that allowing an unauthorised user access to an activated diskette drive could allow that user to introduce a computer virus stored on a diskette; the prior art systems which only prevent access to unauthorised operators once the machine has booted up may have already been contaminated with a computer virus before the operating system password control security system is in operation.

Accordingly the present invention provides a computer system having a power-on password stored in non-volatile memory wherein

This Sheet Has Been Replaced



entry of the power-on password by a system manager permits access to all of the computer functions, thereby permitting the system manager to configure the system, characterised in that at least one additional password is held in non-volatile memory and wherein entry of the additional password by a user permits the system to boot in a manner preselected by the system manager.

The computer system may be a stand-alone personal computer or workstation, or may be linked to other personal computers or workstations and/or mainframe or micro computers by a network.

Suitably there are available a plurality of additional passwords, in particular at least two classes of additional password are provided, each of the classes of additional password providing a different level of security access to the system.

At least one of the different levels of access preferably disables all input devices permitting uploading or downloading of programs or data from diskette, magnetic tape or like storage media, thereby preventing the user from copying material onto or from the system.

In a preferred embodiment of the present invention the power-on password and the additional password(s) are stored as keyboard scan codes in non-volatile CMOS RAM, such as for example battery powered CMOS RAM. The passwords are suitably seven characters in length with a checksum character.

A computer system particularily suited for use of the present invention is a personal computer, such as the IBM Personal System/2 Model 50, 55, 70 or 80 having a diskette drive and a fixed disk.

The preferred configuration of a computer system of the invention is one wherein entry of the additional password causes the diskette drive boot facility or other devices to be disabled. The

This Sheet Has Been Replaced

additional password(s) used in such a system may be stored in non volatile RAM or on a sector of the fixed disk; the sector chosen will be a sector which is not accessed in normal use of the user data on the fixed disc.

As an additional particularily preferred security feature for the computer system, failure by an user to enter a correct password within three attempts causes the system to require the power to be turned off and on again by the user before a further attempt to enter a password can be made.

In a further embodiment of the present invention there is provided a method of configuring a computer system to restrict boot up of the system to a manner preselected by a system manager having knowledge of a power-on password, said password permitting the system manager to access all facilities of the system to enable configuration of the system and installation of appropriate additional password authorisation.

One way of carrying out the invention is described below with reference to the accompanying drawings which illustrate a preferred embodiment of the invention.

Brief Description of the Drawings

Figure 1 is a schematic block diagram of a data processing system on which the invention may be implemented.

Figure 2 is a flow chart of the logical operation of the processor in the operation of an embodiment of the invention having a single additional password.

Figure 3 (divided for convenience into Figures 3a and 3b) is a flow chart of the logical operation of the system in the operation of an embodiment of the invention having two classes of additional

This Sheet Has Been Replaced

password, each of the classes of additional password providing a different level of access to the system.

Description of the Preferred Embodiment

Figure 1 illustrates a typical hardware set-up, such as the IBM Personal System/2 computer, on which the present invention may be implemented. The data processing system comprises a microprocessor 1 such as, for example the Intel 80386 or similar microprocessor, which is connected to a system bus 2, which comprises a set of data lines, a set of address lines and a set of control lines. A plurality of I/O devices including user input means (e.g. a keyboard 3), display 4, printer 5, random access memory 6, read only memory 7, storage media (eg diskette drive 8 and fixed disk 9), are connected to the bus via respective adaptors 10 through 16.

An operating system, such as for example IBM PC DOS or Operating System/2 (Operating System/2 is a trademark of International Business Machines Corporation) may be loaded from the storage media 8, 9 into memory 6 to provide instructions to the microprocessor 1. The loading of the operating system is activated by the boot program held in ROM. The operating system may be loaded from either the fixed disk 9 or from a diskette inserted in the diskette drive 8. Conventionally the system first checks to see whether an appropriate diskette is present in the diskette drive, and if present attempts a load from the diskette; if no diskette is present the system attempts to load from the fixed disk drive or remote device.

An application program subsequently loaded into the system will run in conjunction with the operating system to enable the data processing system to perform the application program tasks.

In the IBM Personal System/2 range of computers the power-on password is held in non-volatile (battery powered) CMOS RAM with an

This Sheet Has Been Replaced

eight byte location allocated to the password and its check character. The microprocessor can only access these eight bytes during the Power-On Self Test ("POST"). Once a password has been installed and POST has been completed the password bytes are locked by a hardware latch, it is not then possible for the processor to access the password bytes. To reset the hardware latch it is necessary to turn off the system power, and then turn it on again. The power-on password is only known to the system manager or similar such control person who in addition has access to the internal physical structure of the system via a conventional keylock to permit opening or closing of the covers on the system unit, and access to the internal components of the system.

Upon switching on the personal computer the processor carries out the normal POST checks, including scanning the available Read Only Memory ("ROM") and Random Access Memory ("RAM").

Referring now to the flow chart of Figure 2, on exiting POST at 20 the system checks at 21 that the security jumper (hard wired switch or contact breaker) on the system unit is closed and, if closed determines at 22 whether the non-volatile CMOS RAM is functioning correctly. Should the non-volatile CMOS RAM not be functioning, for example because the battery powering it has insufficient power, the computer displays at 23 an error message and prevents further input from the user.

Provided the CMOS RAM is functioning correctly the processor checks at 24 whether a power-on password has previously been installed in the CMOS RAM.

The presence of the master power-on password in CMOS RAM at 25 triggers the system to read at 25 a sector of the storage media 9 (Figure 1), in this case the fixed disc, upon which any additional passwords are stored. As an additional security feature the additional passwords are stored in an masked form by applying an

This Sheet Has Been Replaced



algorithm produced from the values contained within the installed master power-on password. The system will be programmed to ensure that an additional password identical to the power-on password cannot be installed.

In addition, at step 26 the computer displays an invitation to the user to enter the (additional) password; should the user wish to change the password a suitable combination of present and desired passwords is entered. The additional password keyed into the system by the user is checked by the system at 27 to determine whether the character sequence is acceptable. The steps of masking and unmasking of the passwords are carried out by conventional methods.

Provided there have been no POST errors 28 which must be dealt with by a user prior to use of the computer, the processor attempts boot up at 29 from a preselected portion of the system's storage media; such storage may include all or part of the fixed disc 9 (Figure 1), or a diskette inserted by the user in the diskette drive 8 (Figure 1). Provided boot was successfully carried out 30, control of those facilities of the system preselected by the system manager is transferred to the user at 31. If boot was unsuccessful for some reason the system repeats operation 29.

An additional security feature is shown on the flow chart at 32. Should the user input an incorrect password at 27 the system permits further attempts: however, only a total of three incorrect entries are permitted at 32. If a third attempt to enter the password is found to be unsuccessful at 32, the system displays at 33 an error message and prevents furthe input from the user until the system has been powered off and on again.

It will be seen from Figure 2 that if the power-on password is disabled (security jumper open at 21) or not installed 24, the system is insecure and boot is possible without entry of a password. The system will, of course, be in this condition until the system

This Sheet Has Been Replaced

manager initially sets up the system and installs the power-on password.

Referring now to the flow chart of Figure 3 which illustrates an embodiment of the present invention having two classes of additional password, each of the classes of additional password providing a different level of access to the system.

The initial steps (20 to 24) in the flow chart are identical to those in the flow chart of Figure 2.

The system reads at 35 (Figure 2) the password sector of the fixed disk and unmasks the security level A and security level B passwords using the master power-on password as the key. A password prompt is displayed at 36 and provided a password, whether level A or B, is entered correctly by the operator and is accepted at 37, progress towards satisfactory boot up continues. The system is programmed to ensure that when multiple passwords are installed, it is not possible for a password character sequence to be repeated.

The number of attempts to enter a password is limited to three by steps 38 and 39.

POST errors are dealt with at 40 and 41.

The system checks at 42 whether a security level A or a security level B password was entered by the user. A security level A user password is a trigger to the system to attempt at 43 the initial boot from a diskette inserted in the diskette drive, whereas a security level B user password triggers the system to attempt at 45 the initial boot from the fixed disk. Successful boot at 43 or 45 allows the system to transfer control to the user of those system facilities selected by the system manager. It will be clear that the holder of a security level B password has a more limited range of access to the system than the holder of a level A password, for

This Sheet Has Been Replaced



example the level B password would be given to a user to ensure that the user could not contaminate the system with a virus held on a diskette.

Should the system not boot successfully from diskette at 44, boot is attempted from the fixed disk at 45 thus permitting the level A password holder access to some but not all of the system facilities the system manager has preselected. Should the system not boot successfully from the fixed disk the system returns to 42.

Reference has been made in the specific embodiments to the operation of the system following power-on; the operation of the system following system reset may be similar or may suitably be blocked to prevent system reset. (System reset for the personal computer is activated by simultaneous depression of the Ctrl, Alt, and Del keys on the keyboard).

Although a particular example of the invention has been described, it will be appreciated that modifications and additions are possible within the scope of the invention.

This Sheet Has Been Replaced

Claims

1. A computer system having a power-on password stored in non-volatile memory wherein entry of the power-on password by a system manager permits access to all of the computer functions, characterised in that at least one additional password is held in non-volatile memory and wherein entry of the additional password by a user permits the system to boot in a manner preselected by the system manager.

2. A computer system as claimed in claim 1 wherein there are available a plurality of additional passwords.

3. A computer system as claimed in claim 2 wherein at least two classes of additional password are provided, each of the classes of additional password providing a different level of access to the system.

4. A computer system as claimed in claim 3 wherein at least one of the different levels of access disables the boot facility of all input devices permitting loading of programs or data from removable storage media such as for example diskette.

5. A computer system as claimed in any preceding claim wherein the passwords are stored in non-volatile RAM.

6. A computer system as claimed in any preceding claim wherein the additional password(s) is stored in a masked form by applying the values contained in the power-on password.

7. A computer system as claimed in any preceding claim having a diskette drive and a fixed disk.

8. A computer system as claimed in claim 7 wherein the additional password(s) is stored on a sector of the fixed disk.

9. A computer system as claimed in claim 7 wherein user entry of the additional password causes the diskette drive boot facility to be disabled.

10. A computer system as claimed in any preceding claim wherein failure by a user to enter a correct password within three attempts causes the system to require the power to be turned off and on again by the user before a further attempt to enter a password can be made.



