Method for Security Partitioning of a Computer System

Background of the Invention

1. Field of Invention

This invention is related to computer systems and in particular maintaining integrity and security of computer networks and data stored on a computer.

2. Description of Related Art

Computers connected to more than one network provide a way for hackers to gain access to other networks connected to the computer and to the data stored in the computer. The hacker generally enters through a lower security network and gains access to a higher security network. A hacker can also gain access to a computer through the Internet. This can allow the hacker to erase or copy stored data.

In US 5,778,174 (Cain) a system is disclosed for providing a secured access to a server connected to a private computer network protected by a router acting as a firewall. The system isolates a public and private network from one another. In US 5,623,601 (Vu) an apparatus and method for providing a secure firewall between a private and public network is discussed. The method produces a transparent firewall with application level security and data screening capability. In US 5,550,984 (Gelb) a security system is disclosed in which two mother boards with network adapters are used to communicate with separate networks. The two mother boards communicate with each other through a transfer adapter and network interface adapter.

In US 5,542,044 (Pope) a computer security device is disclosed having a main and auxiliary storage device. A method for isolating the main and auxiliary storage is described, and the main storage area can be partitioned between a safe storage area and a working area. In US 5,483,649 (Kuznetsov et al.) a computer security system is provided by controlling access to the hard disk controller only through a path using the computers operating system, a modular device driver and the basic input/output system. In US 4,685,056 (Barnsdale et al.) a computer security system is discussed in which a buss is monitored for unauthorized commands or data. Upon detection of unauthorized commands or data, DC power can be disrupted to selected computing devices which are wanted to be protected.

It is usually not practical to isolate all important data resources stored on hard disks in a computer system from outside influences all the time. However, it is practical to make available only those data resources that are needed when connecting to external networks and phone lines, and including connecting only to those networks and Internet providers that are required during a particular computing session. In the process of making some data resources available, the data resources not made available needs to be protected in such away that the active data and networks can not gain access in any way..

SUMMARY OF THE INVENTION

The objective of this invention is to keep data on hard disks and computer network connections not accessible when not being used. In this invention a computer is operated in two or more modes. Data stored in the computer in one mode is not accessible when the computer is

operated in another mode. Similarly a computer network connected in one mode is not accessible in another mode. To accomplish this a computing system is connected to an isolation unit which controls selection of the hard disk drives in the system and controls the connection to external communication lines such as networks and phone lines. The isolation unit contains a control unit in which different computing modes are programmed. Each computing mode selects one or more disk drives by connecting power to the selected drives, and connecting the selected drives to the disk drive interface through the associated buss interface unit (BIU). The BIU associated with the unselected disk drives disconnects the disk drives from the disk drive interface to prevent the unselected disk drives from loading and interfering with signals on the disk drive interface. The connection of external communication lines, including networks and telephone lines, is also controlled by the various modes programmed into the isolation unit. Only those data resources (hard disks, networks and telephone lines) needed for a particular computing mode are powered on and connected to the computing system.

The isolation unit detects when the computer system is powered on or off. When the computer is powered on a computing mode cannot be changed in the isolation unit. The power to the computer must first be turned off and then a new computing mode can be selected. This prevents residual data in main memory, for instance, from being carried over to the new computing mode and the attendant data. Each computing mode powers on at least one hard disk drive and may be connected to one or more external communication lines.

BRIEF DESCRIPTION OF THE DRAWINGS

This invention will be described with reference to the accompanying drawings, wherein:

FIG. 1 is a block diagram of the data security system of this invention;

FIG. 2 is a block diagram of an alternate embodiment of the data security system of this invention;

FIG. 3 is a flow diagram of the method of connecting the isolation unit to a computer and powering on the computer in a computing mode;

FIG. 4 is a flow diagram of an alternate embodiment of the method of connecting the isolation unit to a computer and powering on the computer in a computing mode; and

FIG. 5 is a flow diagram of the method of selecting a different computing mode.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Referring to FIG. 1, an isolation unit 10 is connected to a computer 20. A power supply 21 is connected to a disk drive power bus 22 in the computer 20. The disk drive power bus 22 is connected to a power on detection circuit 11 and switch S4 in the isolation unit 10. The power on detection circuit 11 is connected to the control unit 12 and provides a signal that tells the control unit that the computer 20 is powered on or off. If the computer 20 is off, a computing mode can be manually selected in the control unit 12 by selecting the mode select switch S1. The selected computing mode controls switches S2, S3 and S4. Switch S2 chooses which network to connect to the network adapter 24, and switch S3 connects a telephone line to a modem 23 in the

computer 20. Switch S4 connects power to at least one hard disk drive 26 28 30 32 and its BIU 25 27 29 31. The power to BIU 25 27 29 31 serves as mode selection signals. When the computer power is turned on, the mode selection made manually with switch S1 during power off of the computer connects power to the disk drives selected for the particular mode, connects the selected disk drives to the disk drive interface 33, may connect a network to the network adapter 24 and may connect a telephone line to the modem 23.

Continuing to refer to FIG. 1, mode (1) disk (1) 26 and mode (1) disk (2) 28 including BIU 25 and 27 are connected to mode switch S4, position (a). Mode (2) disk (1) 30 and BIU 29 are connected to mode switch S4, position (b), and mode (N) disk (1) 32 and BIU 31 are connected to mode switch S4, position (n). The BIU's 25 27 29 31 are connected to the disk drive interface 33. When the BIU's 25 27 29 31 are enabled by respective mode selection signals, the BIU's connect the disk drive interface 33 to the powered on disk drives 26 28 30 32. The total number of disk drives is different than the total number of modes, represented by N, by the number of multiple disk drives connected to each computing mode.

An example of the results of selecting a mode can be seen from the connectivity in FIG. 1. When the computer 20 is powered off, mode (1) is manually selected using switch S1 connected to the control unit 12. Selecting mode (1) sets switch S2 to selects network (2) to be connected to the network adapter 24 and switch S3 to not connect a telephone line to the modem 23. Switch S4 connects the disk drive power buss 22 to disk (1) 26, disk (2) 28, and to BIU's 25 and 27. When the computer is powered on, it is brought up in mode (1) with hard disk drives (1) and (2) brought up and connected to the system through BIU's 25 and 27. There is no phone line connected to the modem 23 and network (2) is connected to the network adapter. In order to

connect to a phone line and network (1) to the computer, the computer 20 must be powered off and a new mode selected in the isolation unit 10 that connects the phone line to the modem and the network (1) to the network adapter. This new mode will also select disk drives that may be different from the previous mode.

In FIG. 2 is shown an alternate embodiment of the data security system of this invention. As shown in FIG. 1, an isolation unit 10 is connected to a computer 20. A power supply 21 is connected to a disk drive power bus 22 in the computer 20. The disk drive power bus 22 is connected to a power on detection circuit 11 and switch S4 in the isolation unit 10. The power on detection circuit 11 is connected to the control unit 12 and provides a signal that tells the control unit that the computer 20 is powered on or off. If the computer 20 is off, a computing mode can be manually selected in the control unit 12 by selecting the mode select switch S1. The selected computing mode controls switches S2, S3 and S4. Switch S2 chooses which network to connect to the network adapter 24, and switch S3 connects a telephone line to a modem 23 in the computer 20. Switch S4 connects power to at least one hard disk drive 26 28 30 32.

Continuing to refer to FIG. 2, mode selection signals M11, M12, M2, and Mm are generated by the control unit 12 and connect to BIU 25 27 29 31. The mode selection signals select BIU's corresponding to the selected hard disk drives 26 28 30 32. M11 and M12 enable BIU's 25 and 27 for mode (1) computing and connect hard drive (1) 26 and hard drive (2) to the disk drive interface. M2 enables BIU 29 and connects disk (1) for mode (2) to the disk drive interface 33. In like manner Mn enables BIU 31 and connects disk (1) for mode (N) to the disk drive interface 33. Although not generally desirable, being able to logically disable a disk drive

while powered on can be important in some instances. With the ability to select BIU's separate from the hard disk drives, a disk drive that is powered on could be disconnected from the disk drive interface 33 thereby disabling communications to and from the disk drive without powering it off or other disk drives enabled in the particular computing mode. A possible example of this can be observed from FIG. 2 where in mode (1) both disk (1) 26 and disk (2) 28 are powered on by switch S4 and BIU 25 and 27 are enabled by mode selection signals M11 and M12. If it were necessary and if the control unit 12 were properly configured, either disk (1) or disk (2) could be logically disabled without powering either disk drive down by making a selection in the isolation unit 10 to turn off mode selection signal M11 to disable disk drive (1) or M12 to disable disk drive (2).

An example of the results of selecting a mode can be seen from the connectivity in FIG. 2. When the computer 20 is powered off, mode (1) is manually selected using switch S1 connected to the control unit 12. Selecting mode (1) sets switch S2 to selects network (1) to be connected to the network adapter 24 and switch S3 to connect a telephone line to the modem 23. Switch S4 connects the disk drive power buss 22 to disk (1) 26, disk (2) 28. Mode selection signals M11 and M12 are activated to connect mode (1) disk (1) and mode (1) disk (2) to the disk drive interface 33 through BIU's 25 and 27. When the computer is powered on, it is brought up in mode (1) with hard disk drives (1) and (2) brought up and connected to the system through BIU's 25 and 27. A phone line is connected to the modem 23 by switch S3 and network (1) is connected to the network adapter 24.

Referring to FIG. 3, a method is shown for connecting the computer 20 to the isolation unit 10 using the circuit diagram of FIG. 1. The computer is connected to the isolation unit 40,

and the disk drive power bus is connected to the power on detection circuit 11 and switch S4 in the isolation unit 41. The disk drives and BIU's in the computer are connected to the power selector switch S4 in the isolation unit 42. Networks are connected to the network switch S2 in the isolation unit 43, and the network adapter in the computer is connected to the network switch S2 in the isolation unit 44. The telephone line is connected to the phone switch S3 in the isolation network 45, and the modem 23 is connected to the phone line switch in the isolation unit 46. After all connections are made, the isolation unit is powered on 47. The desired computing mode is selected 49, and the computer is powered on 50. The computer is brought up in the selected computing mode with only the selected disk drives powered on and only the selected networks and phone line connections made. The powering of the hard disk drives and the BIU's through the selector switch S4 provides the enabling signal to connect drives to the disk interface bus.

Referring to FIG. 4, a method is shown for connecting the computer 20 to the isolation unit 10 using the circuit diagram of FIG. 2. The computer is connected to the isolation unit 70, and the disk drive power bus 22 is connected to the power on detection circuit 11 and switch S4 in the isolation unit 71. The disk drives in the computer are connected to selector switch S4 in the isolation unit 72. The BIU's in the computer are connected to mode select signals of the control unit inside the isolation unit 73. Networks are connected to the network switch S2 in the isolation unit 74, and the network adapter in the computer is connected to the network switch S2 in the isolation unit 75. The telephone line is connected to the phone switch S3 in the isolation unit 76, and the modem 23 is connected to the phone line switch in the isolation unit 77. After all connections are made, the isolation unit is powered on 78. The desired computing mode is selected 79, and the computer is powered on 80. The computer is brought up in the selected

computing mode with only the selected disk drives enabled and only the selected networks and phone line connections made. The hard disk drives are powered through the selector switch S4 separately from the BIU's. The BIU's are enabled by the mode select signals from the control unit within the isolation unit. This can allow disk drives to be logically disabled without powering them down.

Referring to FIG. 5, a method is shown for changing the computing mode. Power is turned off to the computer 60 and a new computing mode is selected 61 using the selector switch S1 in the isolation unit 10. After the new mode has been selected, power is turned back on to the computer 62. This procedure of turning the computer power off before selecting a new mode insures that all residual data in memory are erased before the new mode is established on the computer 20, and insures isolation of data between computing modes.

While the invention has been particularly shown and described with reference to preferred embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made without departing from the spirit and scope of the invention.

CLAIMS

1. A computer security system, comprising:

a) a computer system with data elements comprising a plurality of hard disk drives and a means for external communications,

b) an isolation unit connected to said computer system and providing a plurality of computing modes,

c) said computing modes enabling selected hard disk drives and selected external communication.

2. The computer security system of claim 1, wherein an enabled hard disk drive is connected to a hard disk drive interface of said computing system, and a hard disk drive that is not enabled is not connected to said hard disk drive interface.

3. The computer security system of claim 1, wherein a computing mode of said plurality of computing modes can enable one or more hard disk drives.

4. The computer security system of claim 1, wherein a computing mode of said plurality of computing modes can connect a network to said computer system.

5. The computer security system of claim 1, wherein a computing mode of said plurality of computing modes can connect a telephone line to a modem connected to said computer system.

6. The computer security system of claim 1, wherein all external communications can be disconnected from said computer system by a computing mode of said plurality of computing modes.

7. The computer security system of claim 1, wherein computing modes are selected within said isolation unit when said computer system is powered off.

8. A security system for a computer, comprising:

a) a computer with a plurality of hard disk drives,

b) said computer contains external communication interfaces comprising one or more network adapters, modems and serial I/O interfaces,

c) an isolation unit containing a plurality of computing modes connected to said computer,

d) said isolation unit connected to a plurality of external communication lines comprising computer networks and phone lines,

e) said external communication lines connected to said external communication interfaces by means of switches in said isolation unit controlled by a selected computing mode,

f) said plurality of hard disk drives assigned to said plurality computing modes,

g) said isolation unit detects power on of said computer and enables said hard disk drives of said computer according to a selected computing mode.

9. The computer security system of claim 8, wherein a hard disk drive enabled by a computing mode is connected to a hard disk drive interface of said computing system, and a hard disk drive that is not enabled is not connected to said hard disk drive interface.

10. The security system of claim 8, wherein one or more hard disk drive can be enabled by said isolation unit within a computing mode.

11. The security system of claim 8, wherein selection of a computing mode is done when said computer is powered off, preventing previous data in memory from being available to said computing mode.

12. The security system of claim 8, wherein hard disk drives not enabled by a computing mode in said isolation unit are isolated from said computing system.

13 A method to establish security control in a computing system, comprising:

a) connecting a computer to an isolation unit containing a plurality of computing modes,

b) connecting a disk drive power buss of said computer to a mode selector switch of said isolation unit controlled by a selected computing mode,

c) connecting hard disk drives of said computer to said mode selector switch of said isolation unit,

d) connecting bus isolation units of said computer to mode selection signals of said isolation unit,

e) connecting external communication interfaces of said computer to communication selector switches in said isolation unit,

f) connecting external communication lines to said communication selector switches in said isolation unit,

g) powering on said isolation unit,

h) selecting a computing mode,

i) powering on said computer.

14 The method of claim 13, wherein connecting bus isolation units of said computer is done to said mode selector switch of said isolation unit.

15. The method of claim 13, wherein selecting said computer mode selects combinations of hard disks and external communication connections to satisfy a computing requirement while isolating data on other hard disks and networks that are not selected.

16. The method of claim 13, wherein bus isolation units connected to hard disk drives selected by a computing mode are enabled to connect said selected hard disk drives to a disk drive interface in said computer and bus isolation units connected to hard disk drives not selected are not enabled.

17. A method of selecting another computing mode, comprising:

a) turning off power to a computer connected to an isolation unit,

b) selecting a computing mode in said isolation unit,

c) turning on power to said computer.

18. The method in claim 17, wherein selecting said computing mode selects external communication lines to be connected to external communication interfaces within said computer.

19. The method of claim 17, wherein selecting a computing mode is a manual operation.