US005434562A

United States Patent [19]

Reardon

[11] Patent Number: 5,434,562

[45] Date of Patent: Jul. 18, 1995

[54] **METHOD FOR LIMITING COMPUTER ACCESS TO PERIPHERAL DEVICES**

[76] Inventor: **David C. Reardon**, 50 Nottingham, Springfield, Ill. 62704

[21] Appl. No.: **89,637**

[22] Filed: **Jul. 12, 1993**

Related U.S. Application Data

[63] Continuation of Ser. No. 755,866, Sep. 6, 1991, abandoned.

[51] **Int. Cl.**[6] **G07D 7/00**

[52] **U.S. Cl.** **340/825.34**; 340/825.31; 380/4

[58] **Field of Search** 340/825.31, 825.32, 340/825.34, 825.5; 380/4, 25

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,617,650	10/1986	Morino et al.	365/195
4,951,249	8/1990	McClung et al.	340/825.34
4,975,950	12/1990	Lentz	380/4
5,012,514	4/1991	Renton	380/4
5,144,659	9/1992	Jones	340/825.31
5,144,660	9/1992	Rose	380/4
5,289,540	2/1994	Jones	340/825.31
5,313,639	5/1994	Chao	340/825.31

FOREIGN PATENT DOCUMENTS

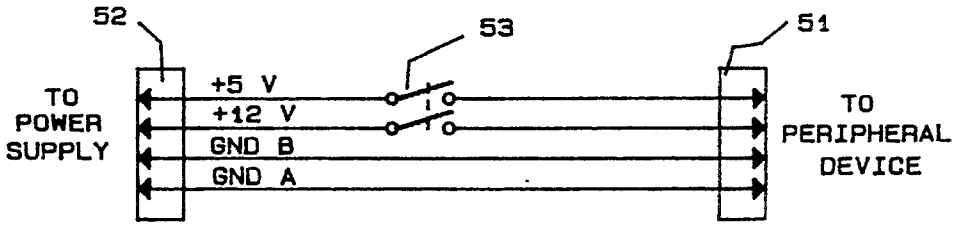
59-128638 11/1984 Japan .

Primary Examiner—Donald J. Yusko
Assistant Examiner—Gregg V. Miller

[57] **ABSTRACT**

One or more user accessible switches are provided by which the authorized user may fully or partially limit the computer's access to one or more of its peripheral devices. The switch inhibits power or control lines to the peripheral device, or enables the programming of access limits to the peripheral device, in a manner which cannot be overridden by the computer. This added level of control allows the user to control the computer's activities so that access to these peripheral devices is allowed only under secure conditions, so as to preclude alteration or destruction of data by unauthorized users or computer viruses. Methods are disclosed by which the switches can render peripheral devices totally inactive, or made to be temporarily read-only, write-only, or write-once in order to implement a number or security protocols for single or multi-user environments.

20 Claims, 1 Drawing Sheet



DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

A Method For Limiting Computer Access to Peripheral Devices

FIG. 1

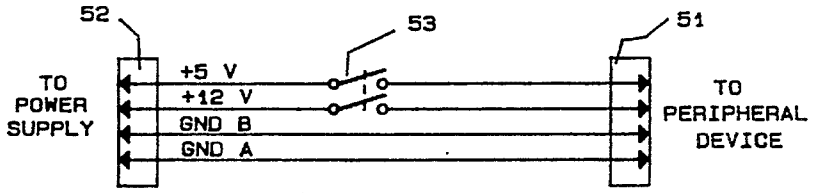


FIG. 2

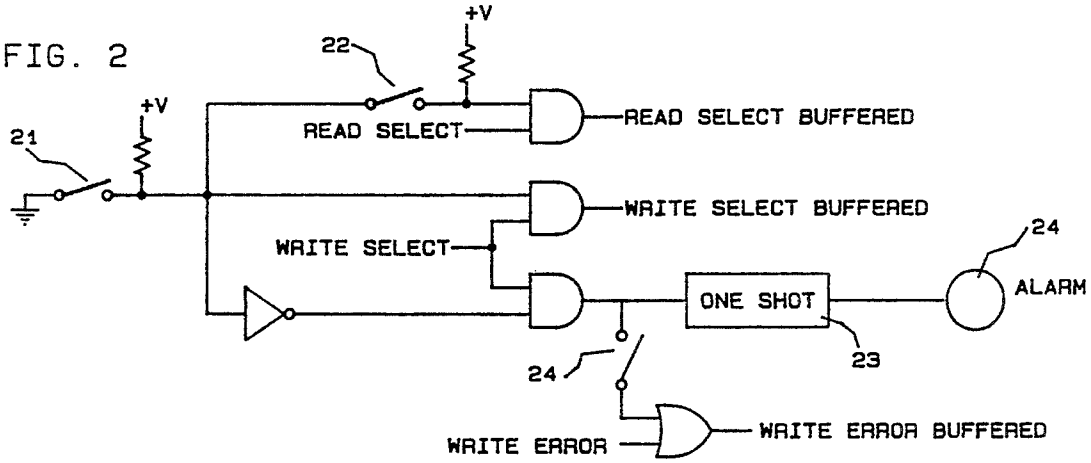
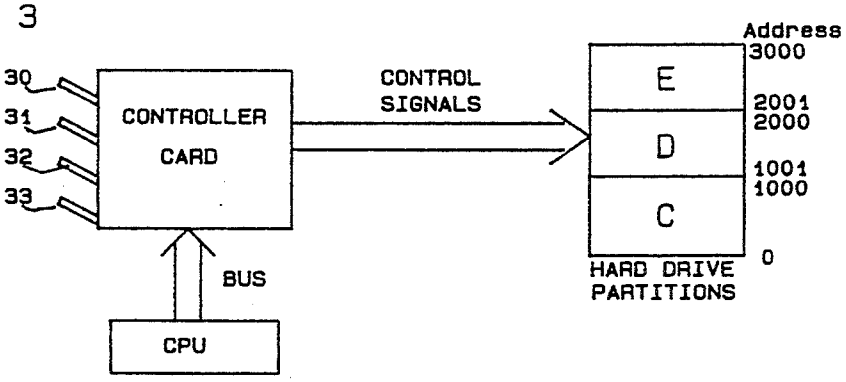


FIG. 3



DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

METHOD FOR LIMITING COMPUTER ACCESS TO PERIPHERAL DEVICES

This application is a continuation of patent Ser. No. 07/755,866, filed Sep. 6, 1991, now abandoned.

BACKGROUND—FIELD OF INVENTION

This invention relates to computer security measures and to the prevention of unauthorized reading or altering of computer data by individuals or programs operating on a computer. Specifically, this invention describes a means and process by which the authorized user of a computer can protect data and programs stored in peripheral devices, such as mass storage media, from alteration or deletion by malicious persons, or computer "virus" programs, or accidents initiated by unskilled persons. This end is achieved by providing the authorized user with a switch whereby the user can completely or partially disable the peripheral device without disrupting the operation of the computer or other peripherals. Alternatively, the switch may disable write access to the peripheral device, such as a widely used computer harddrive, but allow the device to be read.

This invention is particularly useful in multi-user environments, such as those in a university computer lab, wherein only a computer supervisor is authorized to add programs and data to a mass storage peripheral device and other users are authorized only to read programs and data from the storage device. In this example, the computer supervisor would have a key with which he could gain access to write new information onto a harddrive and then could "lock out" write access so that students would be unable to accidentally or maliciously load a "virus" program onto the computer system.

This invention is also useful for persons who desire to evaluate new software but are afraid that by doing so they will be exposing their computer system to infection with a computer virus. By locking out write access to their computer's harddrive, the system is "safe" and the suspect program can be run without risk of it causing an infection which may later cause loss or disruption of programs and data.

By providing complete user control over a computer's access to its peripheral devices, this invention allows the user to implement greater security precautions against unauthorized programs or users. These options include limiting read and write access to the peripheral device, and the ability to configure the peripheral device so as to make all or portions of the device appear to the computer as a read-only, write-only, or write-once peripheral device.

Background—Description of Prior Art

Protecting computer data and programs from unauthorized copying, destruction, or alteration is a major concern for governmental agencies, businesses, educational institutions, and individual users. In addition to protecting valuable data from spies or malicious programmers, there is a need to protect data from computer "virus" programs which can infect a system and cause damage at some later date.

Numerous computer security programs have been written to provide a large variety of features to protect computer data. These include such features as password protection, restricted access to specified files, limited menu options, checksum verification, and scanning for known virus programs or virus-like activities. The major shortcoming of these computer security programs is that they must operate within the computer's working memory space, its RAM. This means the security software is susceptible to other forms of software which can defeat the programs security measures.

The distinct advantage of the present invention is that it is a hardware security device which cannot be bypassed or defeated by software or keyboard programming.

Another advantage of the present invention is that it would allow the computer to be booted from a floppy and used as a floppy disk system, by either totally or partially inhibiting the hard drive. This feature may be of special interest in some multi-user situations.

For example, in a home environment, a father could lock out the harddrive so as to allow his children to boot up the computer and run games from a potentially "virus" infected floppy disk without risk that child or "virus" will intrude upon or damage any of his business programs or files on the hard drive.

Similarly, in a university setting, the present invention could be used to make the mass storage media "read only," thus allowing the students to read necessary data and programs from the hard drive but block out any attempts to write to the hard drive, thus forcing all student created files and documents to be stored on removable floppy diskettes. Alternatively, this process could be implemented to provide read only access to a protected portion of the harddrive which contains the executable programs and allow write access only to an unprotected portion of the harddrive dedicated to data storage.

SUMMARY OF INVENTION

The object, advantages, and features of the present invention are:

(a) to provide a computer user with a method for protecting a computer's security software from probing, alteration, bypass, or deletion;

(b) to provide a computer user with a method for protecting a computer's mass storage media from corruption by an unauthorized user or computer "virus";

(c) to provide user accessible switches by which the user can restrict the computer's access to all or portions of computer's peripheral devices.

(d) to provide an alarm means to notify users of an unauthorized attempt to write to a computer's peripheral devices, wherein such an attempt may indicate that a computer virus-like activity is taking place.

These and other objects are accomplished in accordance with the present invention by providing one or more user activated switches, which may be of a key-locking type, which totally or partially disable the computer's access to peripheral devices such as mass storage media or network communications.

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 is a schematic drawing of a power interception circuit between a host computer's CPU and a peripheral mass storage device.

FIG. 2 is a schematic drawing of electronic circuit which can block all write accesses to a typical personal computer's harddrive whenever selected to do so by a user activated switch.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

FIG. 3 is a block drawing which shows the relationship between a peripheral device such as a harddrive, the peripheral's controller card, and access switches which limit the computer's access to the peripheral device, and the computer's central processing unit.

DESCRIPTION OF INVENTION

For the purpose of this discussion, peripheral devices shall mean any device external to the central processing unit (CPU) of a computer, including mass storage media devices such as hard disk drives and their controllers, computer network interface cards, and other I/O devices. The term controller card refers to the electronics associated with the peripheral device which interface the device with the host computer, interpret the host computer's commands, and controls the peripheral devices activities, this controller card circuitry may be embedded in the peripheral device or remotely situated and in communication with the peripheral device. The term computer virus, or simply virus, refers to any potentially destructive computer program which may cause malfunction of the computer, corruption of files, loss of data, or other unwanted and unexpected results. The term unwanted memory loss refers to the condition of damaged, lost, or altered memory locations due to computer virus activity or accidental or malicious damage caused by person with access to the computer.

This invention describes a means and process by which to disable the computer's access to all or part of a computer's memory system or associated peripherals, so as to protect the computer from computer virus infections when using new or untested software. In addition, this invention can prevent erasure, alteration, or other damage to files stored on a harddrive or network due to accidental, negligent, or malicious behavior of persons with access to the computer.

The present invention achieves these ends by totally or partially disabling access to peripheral devices which may be subject to unwanted memory loss, typically these are mass storage media devices such as a harddrive. Typically, the disabling of the peripheral device is executed by the user operating a switch, which may be of a keylocking type, which fully or partially disables the peripheral device as long as the switch is activated. While this invention can be realized in many configurations which are familiar to persons practiced in electronics, six principle methods for implementing of this device are illustrative of the scope of this invention. The switch may be configured to either

1) physically disconnect the power supply to the mass storage media device and/or the communication link to the network;
2) physically disconnect control lines to the mass storage media device so as to disable all writing functions; or
3) activate an electronic signal which would electronically disconnect, block, or buffer control signals to or from the harddrive and/or network interface so as to selectively block write activity to all or part of the harddrive or network.
4) activate an electronic signal which would be detected by the peripheral device's controller which would then fully or partially disable portions of the peripheral device according to the predetermined definition associated with that switch.
5) activate an electronic signal which would be detected by the peripheral device's control processor which would then enable the configuration and storage of configuration data which would fully or partially disable the CPU's access to portions of the peripheral device.
6) activate an electronic signal which would be detected by the CPU and would enable sections of the BIOS code stored in firmware whereby this BIOS code would fully or partially limit access to at least on peripheral device.

The following discussion describes these various embodiments in greater detail.

EMBODIMENT 1

The simplest, but least selective, means for achieving the ends described above is shown in FIG. **1**. This drawing shows a means for intercepting and interrupting the power to a typical harddrive peripheral device in a common variety of personal computers. In this typical example, the harddrive receives its power from a four pin connector to the computer's central power supply. Normally, the harddrive is powered on whenever the computer is on, and powered off whenever the computer is off. If, however, the harddrive is connected to connector **51** in FIG. **1**, and the computer's central power supply output is connected to connector **52**, then the user can selectively poweroff the harddrive by switching switch **53** to the disconnected position without disrupting the computer's normal operation. As long as switch **53** is in the disconnected position, the computer can be used, even with computer virus infected software, without risk of infecting or damaging information stored on the harddrive.

Switch **53** may be of a key locking type which is positioned in some accessible location so that the user can conveniently reach it.

In a typical application, a parent who uses a home computer for business applications may use this invention to turn off the harddrive and lock it out so that children may experiment with the computer and operate new, unusual, and highly suspect programs, without risk of damaging important business information.

In another typical application, a computer user who enjoys experimenting with new software traded among friends or loaded down from electronic bulletin boards, can use switch **53** to safeguard his harddrive from computer viruses while at the same time enjoying the indiscriminate use of programs which come from unknown or suspicious origins.

EMBODIMENT 2

The same ends can be achieved with a slight variation on the power switching method illustrated in FIG. **1**. In this variation of the present invention the switch would physically disconnect the control lines to or from the peripheral controller. Typically this would involve the ability to disconnect the device select, write select lines, or other access signals which the controller uses to enable access to the peripheral device. When one or more of these control signals is disconnected, the computer would be able to run normally but would not be able to write information to the peripheral device.

EMBODIMENT 3

A more expensive, but more selective, means of achieving the above goals would involve the electronic switching of control signals to the peripheral device. An example illustrative of this means is shown in FIG. **2**. This embodiment of the present invention would allow the user to selectively disable write access to a

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

peripheral device such as a harddrive, while selectively maintaining the option to read data from the peripheral device. In addition, this electronic means demonstrates two optional features which would aid in the testing of software to identify the existence of computer viruses.

As shown in FIG. 2, switch 21 is used to alter an electronic logic level which is logically AND'ed with the normal write select signal to the peripheral device, such as a harddrive. When switch 21 is in the open position, a logical 1 is generated and the computer has normal access to the peripheral device. When switch 21 is in the closed position, a logical 0 is generated, the write select signal is blocked, and the all write access to the peripheral device is inhibited.

For the purpose of identifying improper user activity or the presence of a computer virus, it may be desirable to alert the user that a write command was attempted whenever switch 21 is in the closed position. For this purpose, the inverted signal from switch 21 is logically AND'ed with the write select signal to trigger a retrigerable oneshot logic device, 23, which in turn would sound the alarm, 24, for a minimum period of time.

As an additional option, the oneshot 23 could be configured to beep the alarm a single time whenever switch 21 is activated in order to audibly notify the user that the "quarantine" has been initiated. Another alternative would be to provide an LED which would remain lit whenever switch 21 is closed in order to provide a visual indicator to the user that write access to the harddrive is blocked and the "quarantine" is active. Neither of these two options are illustrated in FIG. 2.

Normally, the optional switch 22 in FIG. 2 would be left in the open position so that whenever switch 21 is in the closed position, the computer would have normal read access to the peripheral device but would not be able to write to it. However, in some circumstances the user may wish not only to protect the peripheral device from alteration but also wishes to lock out others from examining its contents. Switch 22 is provided for this circumstance. If it is desired to configure the electronics to also block read access to the peripheral whenever switch 21 is in the closed position, switch 22 is set to a closed position.

FIG. 2 also illustrates one additional optional feature, namely a feedback write error signal to the computer, or the peripheral's controller. In a typical application where the write select to a harddrive is blocked, the computer may think that it is successfully writing data to the harddrive. This may be a useful feature for tricking a computer virus into believing that it is successful in its write attempts. However, in some applications it may be desirable to alert the computer, and thereby the user, that write access is being blocked so that they can take corrective measures if necessary. Therefore, if a write error signal is desired, the inverse signal from switch 21 can be logically AND'ed with the write select signal to produce a logical 1 whenever a disallowed write attempt is made, which in turn can be logically OR'ed with the normal write error signal which is provided from the peripheral device so that the computer or controller will be notified that the write attempt did not succeed. Other control signals can be similarly controlled for similar or varied effects which achieve the same function of protecting data on the harddrive in all or some locations.

The circuitry of this embodiment could be added to the controller card for the peripheral at little cost during the time of design and manufacture. Alternatively, this circuitry could be placed on a separate expansion card as is typically used in personal computers, with the control cable extending from the controller card, which would normally be plugged directly into the peripheral device, being plugged instead into this separate expansion card. Another control cable, including the intercepted and buffered control signals, would then extend from the separate expansion card, containing the circuitry described in this embodiment of the present invention, to the peripheral device.

This embodiment of the present invention serves all of the above stated purposes but can also be used in additional applications. For example, a computer supervisor in a business could lock out write access to the harddrive so that staff can use the programs on the harddrive but not load unauthorized programs onto the harddrive. Users would be forced to save data files to unprotected media, such as diskettes. In another application, an individual can temporarily "quarantine" the harddrive by making it "read-only" while evaluating new software which may be infected with a computer "virus."

EMBODIMENT 4

FIG. 3 represents another embodiment of this invention which is illustrative of the scope of the invention. In this embodiment, the electronics and microcontrollers already present on the peripheral device's controller card would directly read and interpret the switches to carry out the processes disclosed in this invention. This arrangement is especially beneficial since it adds little or no cost to the consumer and manufacturer, and at the same time provides the user with increased flexibility in controlling access to all or part of the peripheral device.

The typical controller card is already capable of interpreting commands from the computer and implementing the appropriate read and write functions to the peripheral device. Typically, these actions of interpreting commands and implementing responses are under the control of a predefined logic circuit or a programmable microcontroller which operates a program from its fixed memory. In order to implement the present invention most effectively and at least cost, only a slight modification of the controller card is necessary. This modification would involve the addition of one or more switches which are read into the controller card's circuitry as additional control or configuration signals. The means for implementing the reading of these switches, and logically combining them to produce the desired results in either hardware logic or firmware programs are standard practices for all electronic and software designers, therefore no detailed explanation for the buffering of the switch signals is necessary.

These switches, may be of a toggle or key locking type, or may be implemented as a bank of miniature DIP switches in cases where there are a mutiplicity of options to partially disable access to the peripheral, or a combination of the above. In the typical application, these switches would be in a location easily accessible to the user on the outside of the computer. These switches might be advantageously located for accessibility on the front panel of the computer case, near or on the face of the harddrive, for example, or they may be placed on the cover plate for the controller card which fits in an expansion slot, such as is common for IBM-compatible computers. Other locations of convenience would be immediately obvious to computer and peripheral device designers.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.