United States Patent [19]

Hwang

[11] **Patent Number:** 5,960,172

[45] **Date of Patent:** Sep. 28, 1999

[54] **DIGITAL COMPUTER SYSTEM SECURITY DEVICE**

[75] Inventor: **Seung-Hwe Hwang**, Kyungki-do, Rep. of Korea

[73] Assignee: **SamSung Electronics Co., Ltd.**, Suwon, Rep. of Korea

[21] Appl. No.: **08/777,067**

[22] Filed: **Dec. 30, 1996**

[30] **Foreign Application Priority Data**

Dec. 30, 1995 [KR] Rep. of Korea 95-68217

[51] **Int. Cl.⁶** **H04F 1/00**
[52] **U.S. Cl.** **395/186**; 380/25
[58] **Field of Search** 395/186, 187.01, 395/188.01; 380/3, 4, 23, 25

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,103,221	4/1992	Memmola .
5,202,997	4/1993	Arato .
5,261,070	11/1993	Ohta .
5,311,591	5/1994	Fischer .
5,355,414	10/1994	Hale et al. 380/25
5,369,394	11/1994	Quirk et al. . .
5,388,211	2/1995	Hornbuckle .
5,434,562	7/1995	Reardon .
5,454,032	9/1995	Pinard et al. 379/167
5,465,341	11/1995	Doi et al. . .
5,481,253	1/1996	Phelan et al. . .
5,542,045	7/1996	Levine .
5,548,721	8/1996	Denslow .
5,610,981	3/1997	Mooney et al. 380/25

Primary Examiner—Albert DeCady
Attorney, Agent, or Firm—Robert E. Bushnell, Esq.

[57] **ABSTRACT**

A security device for a digital computer system having a peripheral device and peripheral device controller, includes a security user input/output unit which displays the contents stored in the peripheral device and receives the information for the protection of the peripheral device, a security system controller which is connected to the security user input/output unit, and protects and controls the peripheral device, and a security controller which is connected to the security system controller, the peripheral device controller and the peripheral device, and protects the peripheral device from being controlled by the peripheral device controller to provide a security device operated under another operating system by using hardware, thereby allowing a computer system to interface with an input/output device or a file in a normal state while the security device protects the computer system.

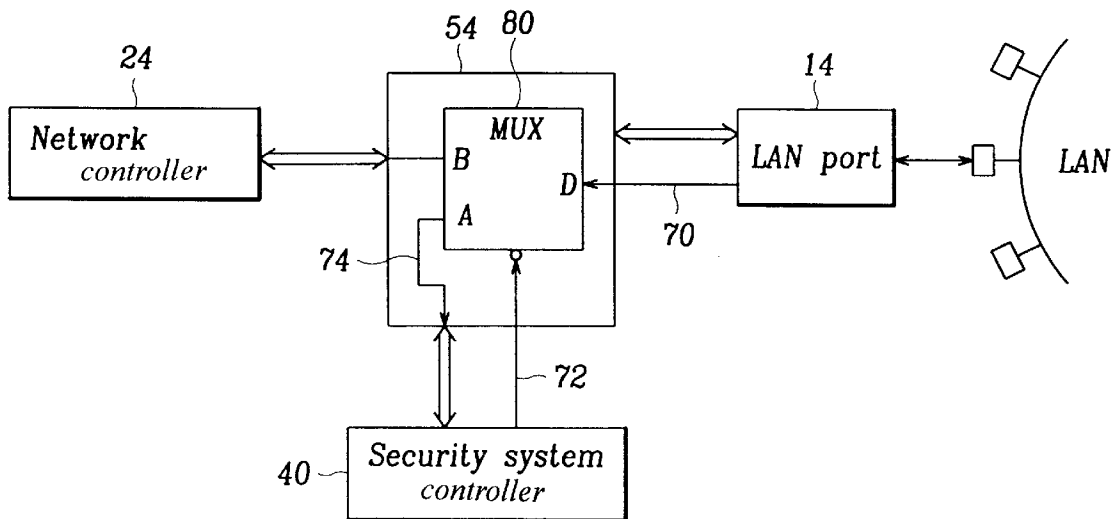**20 Claims, 3 Drawing Sheets**
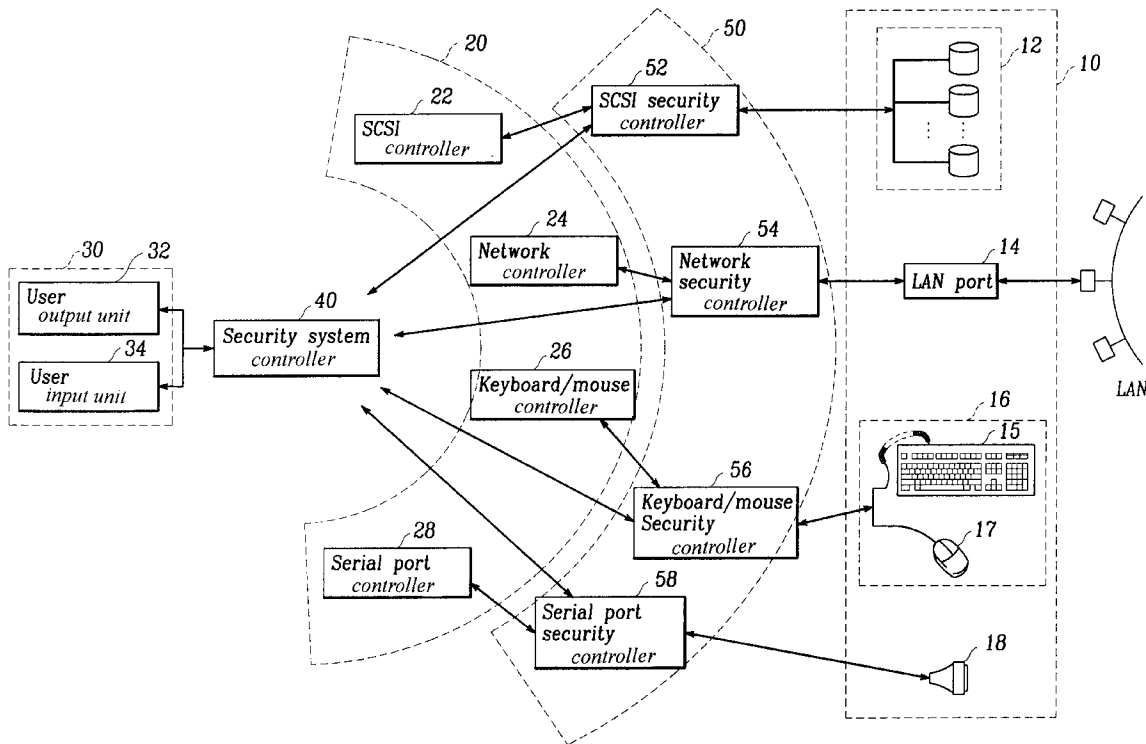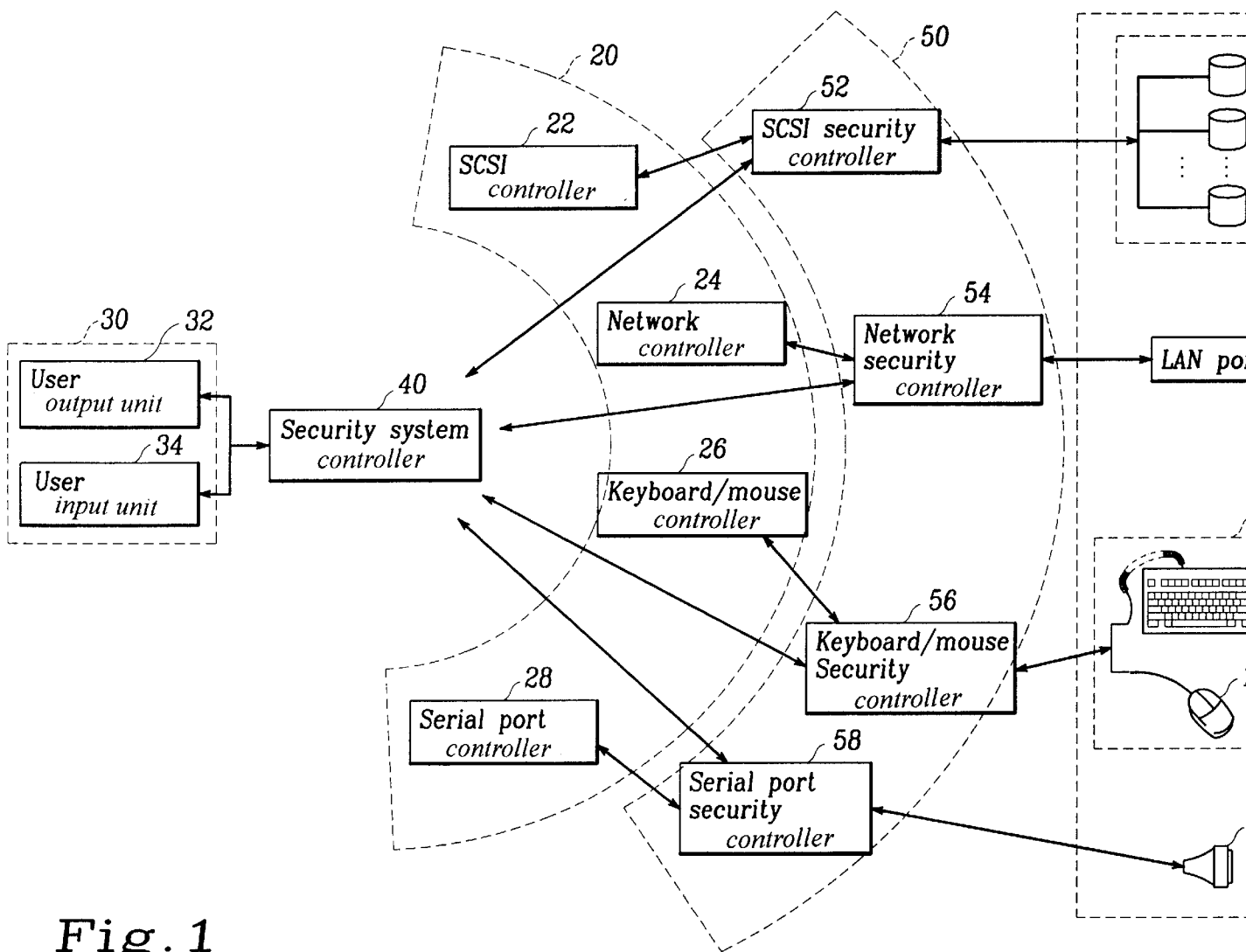
Fig.1
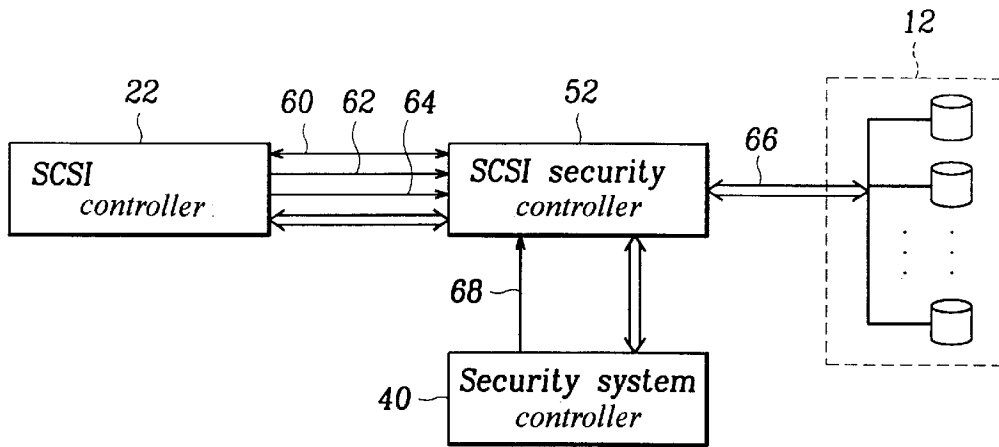
Fig.2
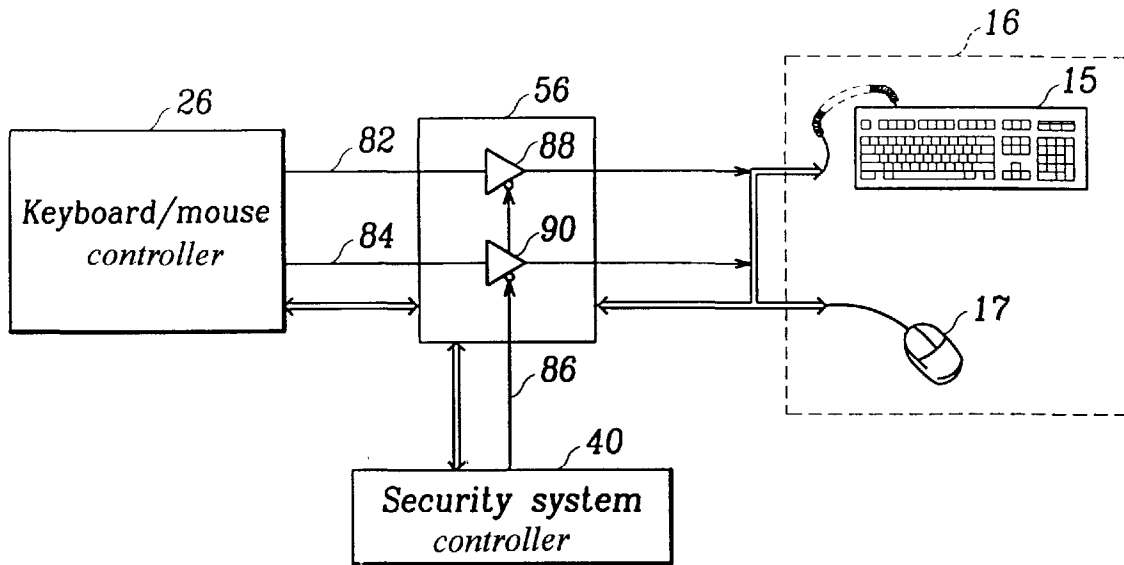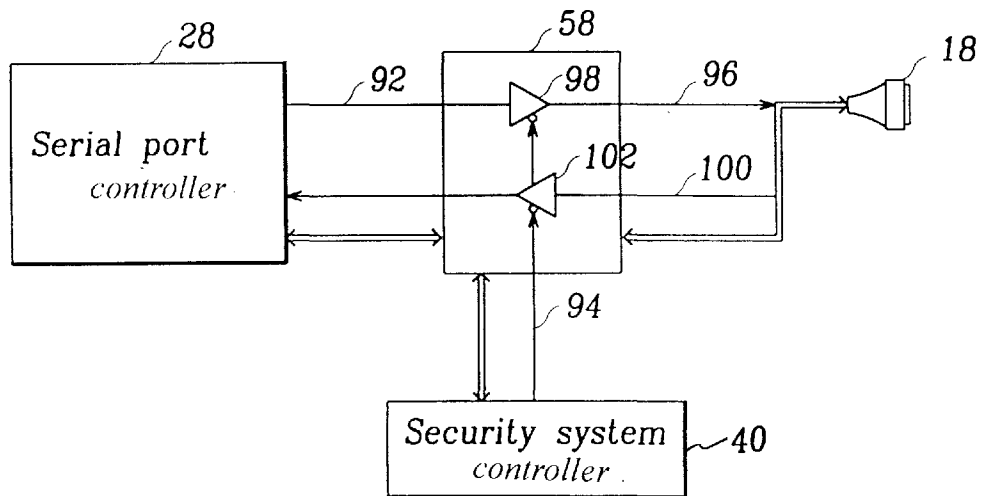

Fig.3

Fig.4

Fig.5

DIGITAL COMPUTER SYSTEM SECURITY DEVICE

CLAIM OF PRIORITY

This application make reference to, incorporates the same herein, and claims all benefits accuring under 35 U.S.C. §119 from an application Entitled Digital Computer System Security Device earlier filed in the Korean Industrial Property Office on Dec. 30, 1995 and assigned Ser. No. 95-68217.

FIELD OF THE INVENTION

The present invention relates to a security device for a computer system, more particularly, to the security device which can be operated under a different operating system. The present invention allows a computer system to interface with an input/output device or a file in a normal state while the security device protects the computer system.

BACKGROUND OF THE INVENTION

The notion of controlling access to computer peripherals via a separate operating system is not new. For example, U.S. Pat. No. 5,434,562 for a Method For Limiting Computer Access to Peripheral Devices to Reardon discloses the use of user operated hardware switches to deny access to peripheral devices. Access to the switches can not be over-ridden by the computer. The purpose of this arrangement is to prevent unauthorized users or computer viruses from gaining an access to peripheral devices. Reardon '562, however, appears to contain solely mechanical switches without any software to operate them.

Another example is found in U.S. Pat. No. 5,202,997 for a Device For Controlling Access to Computer Peripherals to Arato. A microprocessor requests the user enter a valid identification code in order to gain access to a peripheral. When the user inputs an unauthorized code, the microprocessor will deny access to the peripheral. Arato is an example of software being used to provide security access to computer peripherals.

A similar example is found in U.S. Pat. No. 5,481,253 for an Automotive Security System to Phelan et al. discloses an anti-theft system includes a microprocessor based control module that enables operation of solenoids of the power circuits of the car only if a proper identification code is entered.

Finally, U.S. Pat. No. 5,311,591 for a Computer System Security Method And Apparatus For Creating And Using Program Authorization Information Data Structures to Fischer discloses a program authorization information required to gain access to various terminals. This is to prevent viruses from potentially destroying devices by moving from terminal to terminal. The co-signatory authority may be required in one embodiment as a security measure to prevent unauthorized access to devices.

What is needed is a hardware switching security device that is controlled by software operated under a different operating system so that access to and from peripheral devices may be controlled.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a security device for a digital computer system, operated under a different operating system by using hardware, that protects a computer system while allowing it to interface in a normal state with an input/output device or a file.

These and other objects may be achieved by having a security device for a digital computer system having a peripheral device and peripheral device control means that includes a security user input/output means which displays the contents stored to the peripheral device and receives information for the protection of the peripheral device, a security system control means which is connected to the security user input(output means, and protects and controls the peripheral device, a security control means which is connected to the security system control means, the peripheral device control means and the peripheral device, and protects the peripheral device from being controlled by the peripheral device control means.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete appreciation of the invention, and many of the attendant advantages thereof, will be readily apparent as the same becomes better understood by reference to the following detailed description when considered in conjunction with the accompanying drawings in which like reference symbols indicate the same or similar components, wherein:

FIG. **1** is a schematic diagram of a digital computer system security device in accordance with the preferred embodiment of the present invention;

FIG. **2** is a security schematic diagram of a hard disk drive of the digital computer system security device in accordance with the preferred embodiment of the present invention;

FIG. **3** is a security schematic diagram of a LAN port of the digital computer system security device in accordance with the preferred embodiment of the present invention;

FIG. **4** is a security schematic diagram of a keyboard/mouse of the digital computer system security device in accordance with the preferred embodiment of the present invention; and

FIG. **5** is a security schematic diagram of a serial port of the digital computer system security device in accordance with the preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

In order to protect computer system from an unauthorized access, a screen locking system which interrupts the input of a keyboard and a mouse and a key locking system which restricts the operation of the computer system if the user does not press a set key when booting is used.

Many operating systems are used in one computer system because of the increase of the uses and applications for the computer. Under these systems, the above protecting methods are generally used.

In the above prior art, if the protector is not removed, the user can not use the entire computer system. Also, the above method which is used under one operating system can not be used in another operating system.

A preferred embodiment of the present invention will become apparent from a study of the following detailed description with reference to the accompanying drawings.

As shown in FIG. **1**, the security device for a digital computer system having peripheral devices **10** and peripheral device controller **20** which controls the peripheral devices **10**, includes a security user input/output unit **30** which displays the contents of peripheral devices **10** and receives information for the protection of the peripheral devices **10**, a security system controller **40** which is connected to the security user input/output unit **30**, and protects

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.