Annales UMCS Informatica AI 2 (2004) 323-329

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI

http://www.annales.umcs.lublin.pl/

Simple hardware method of data protection

Jerzy Kotliński*

Institute of Physics, Maria Curie-Skłodowska University,
pl. M.Curie-Skłodowskiej1, 20-031 Lublin, Poland

Abstract

A rapid development of the antivirus and antispy software makes us realize how the threat of unauthorized exploring of computer data has been increasing in the recent few years. It is evident, that new generation of spyware has the ability to penetrate computer data through a network. The author suggests that untypical structure of hardware can improve security of data. In this paper the idea of hardware protection of data and additional hardware components: switches of the hard disk and the network card are described.

1. Introduction

The problem of data security connected with computer hacking and data penetrating is growing simultaneously with the computer network expansion.

The common way of data protection is using of special software. Protective programs are effective when the attack is made in a well-known way. Each new generation of spyware can usually make an effective attack.

The susceptibility to the network attack is caused by the fact, that the hardware and soft-ware of a typical computer as well as system bugs are known. The author of the present work has decided to defend against external, network attack by creating untypical hardware structure of computer. This structure cannot be known to the attacking side (of course, no longer after the moment of publication of this paper).

2. Principles of a project

A method of the computer data security improvement described in the present paper is based on two trivial assumptions:

- it is not possible to read the data from disk which does not exist;
- it is not possible to transmit the data if the connection between computer and network is broken.

* *E-mail address*: jotkot@tytan.umcs.lublin.pl

During the computer start-up BIOS software and operating system test computer hardware. Devices which answer in the appointed time are registered in a list of computer equipment. Not registered devices are not allowed to begin standard operation. It is possible to reduce a number of active devices by physical removing or making of their work incorrect in the computer system. So, it is possible to increase or decrease a number of active devices in computer by switching them on or off (if, of course, devices are equipped with such switches).

The presented method is based on 'selective virtual damaging' of devices without causing real physical failure. With regard to safety of the computer it was decided, that every switching of the state of devices should be made before starting-up the computer and not during its normal operation.

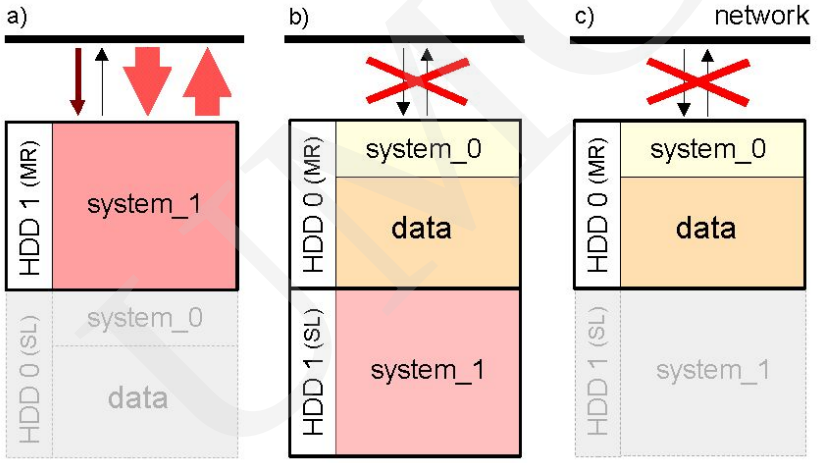

Fig. 1. Scheme of configuration of HDD disks in computer for different modes of operation: with network (a) and without network (b, c)

The scheme of configuration of computer disks for different modes of work is shown in Fig. 1. The configuration can be made by activating or disactivating the network card and HDD disks with declaration of their status (master or slave). The computer in Fig.1a is adapted for operation within network. In Fig. 1b and Fig. 1c the computer adapted to work without a network is shown. The protected data should be stored on the HDD0 disk.

In configuration for network operation (Fig. 1a) the network card and HDD1 disk are activated. In this mode the HDD1 disk works as MASTER. On the HDD1 disk an operating system called 'system_ 1' is installed. In the presented case the HDD0 disk is inactive and switched to SLAVE mode.

The work without network (Figs.1b and 1c) is possible in the case of the lack of network card. In this case the network card exists but it is not active. The operating system called 'system_ 0' is installed on the active HDD0 disk which

works in MASTER mode. The HDD1 disk can be included into the system (Fig. 1b) or not (Fig. 1c). It each case the HDD1 disk works as SLAVE.

In the case of infection of the operating system stored on HDD1, the penetrating software can operate on the HDD1 disk only. The HDD0 disk cannot be directly infected. If the infection transfers onto an operating system which is stored on the HDD0 disk, the penetrating software will not have a chance to work on-line, because connection between computer and network does not exist.

All the considerations presented above can be expressed in several postulates, which define a new structure of the computer:

- the computer should work correctly in the network and without it;
- the computer should have the untypical hardware system of data protection:
  - in the mode of operation without network the full access to protected data should be enabled – the network connection should be hardware blocked,
  - in the mode of operation with network the computer should not have an access to protected data – the access to the hard disk with protected data should be hardware blocked,
- the selection of operating mode should be very easy and should be made before starting of the computer,
- all applied changes should not disrupt the standard structure of the computer and should be easily removable.

The above mentioned principles determine new organization of software and hardware. One can say, that after adaptation the computer contains two independent computers which are placed in a common casing**.**

The modernization of the computer requires 3 additional units:

- a mechanical switch for selection of the operation mode;
- a switch of HDD disks;
- a switch of a network card.

A construction of the HDD switch should make possible switching between MASTER and SLAVE modes and the physical separation of the hard disc from the EIDE bus possible.

A construction of the network card switch should guarantee its full cutting off from the PCI bus.

2. The enable/disable switch of the Ethernet card

The physical separation between network and computer can be made in two ways. The first way depends on disconnecting of the network cable from card. The second one depends on deactivating of the network card in computer hardware. In spite of the simplicity, the first way is difficult to realize, because of a floating potential of the network wires. Bad construction of switch can introduce a distortion of signal into network and can disturb the network work.

The second way depends on deactivating of the network card in computer. Network cards produced at present are usually connected with a computer by the PCI bus. In Fig.2a the typical plot of transmission on the PCI bus is shown [1]. A target device is pointed by the PCI address, the PCI order and 'FRAME' signal. Actually selected device has to confirm a call by the signal DEVSEL.

a) b)

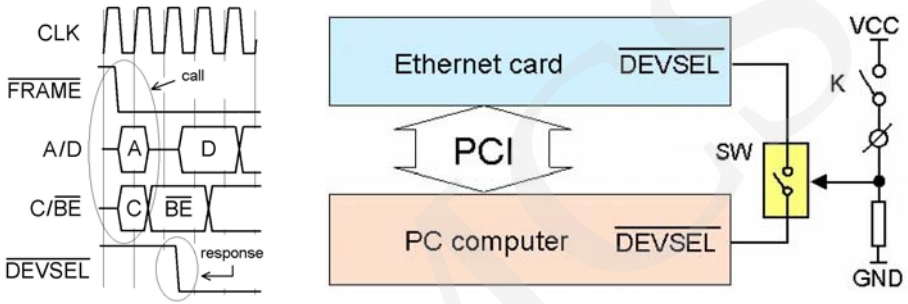

Fig.2. Typical plot of transmission on the PCI bus (a) and the place of modifying of the network card (b)

The lack of this confirmation can be recognized as the busy or defect state of the selected device or as the absence of device in the system. It is sufficient to break the DEVSEL line and computer would treat the network card as not present in a system. This modification can be made on the network card directly.

3. The enable/disable switch of the HDD disk

The switch of the hard disk should provide the connection or disconnection of disk from the EIDE bus. It should also provide a choice of the disk status in a system (master or slave). The switch cannot disturb work on the EIDE bus – the impedance of signal lines of the bus should be compatible with the standard system without the switch. In the prototype circuit the switch of the HDD disk was made as an intermediate unit placed between the HDD disk and the EIDE cable.

Fig. 3 presents the scheme of the HDD switch. Figs. 4a and 4b show the prototype module of the HDD switch (a) and its placement in computer (b).

In order to control the HDD switch only two binary signals are necessary. These signals are labeled in Fig. 3 as CS0 and CS1. For an externally defined logical level of the CS0 and CS1 signals a required action of the HDD switch can be obtained by suitable setting of the SW, SW1 and SW2 switches. The CS0 signal is dedicated for switching the hard disk ON/OFF and its logical state can be changed by the jumper switch SW. The CS1 signal is designed to define the HDD status: MASTER or SLAVE. The exchange of the CS1 logical level can be

made by suitable placing the SW1 and SW2 connectors onto MR and SL pins which are placed on the rear side of the HDD box.

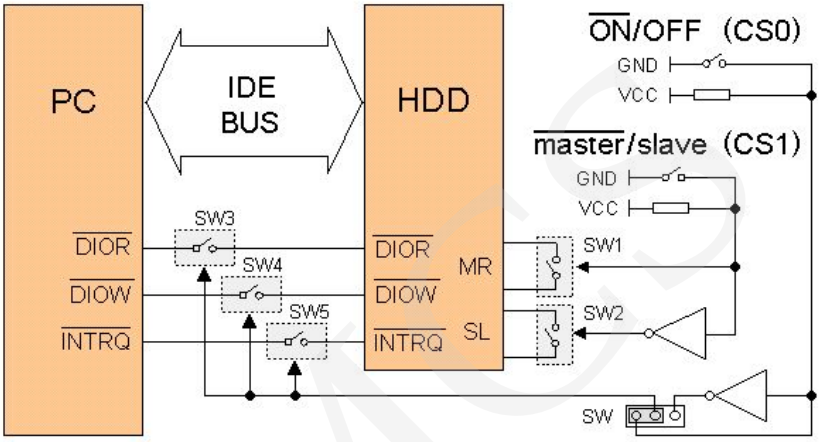

Fig. 3. Circuit scheme of the HDD switch

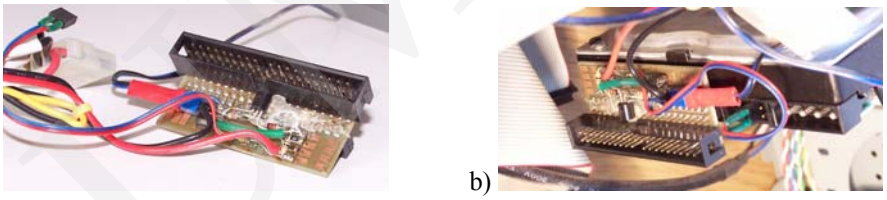

Fig. 4. Module of the HDD switch (a) and its placement in the computer (b)

4. A mode switching of the PC

It was mentioned above that only two binary signals are necessary to control the HDD switches. For disconnecting of the network card only one control signal is required. Fig. 5 presents a full scheme of connections in the modernized computer.

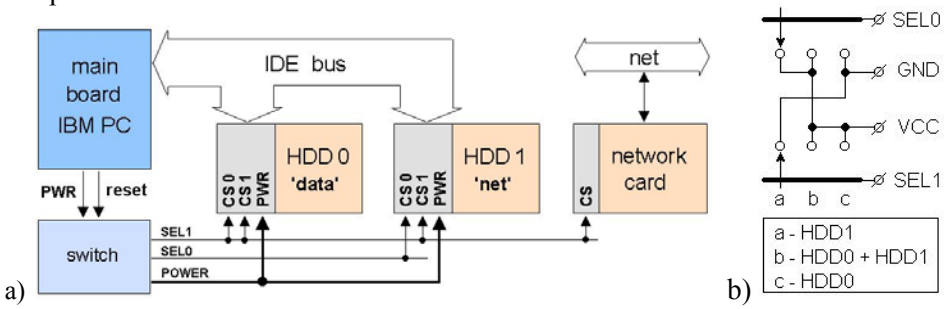

Fig. 5. Scheme of control connection of the HDD disk and network card switches (a) and scheme of mechanical switch (b)

The state of the switch which will generate the CS0 and CS1 signals decides about the mode of the computer operation. The switch can be an electronic one and stores settings at the moment of the computer start (by the use of the RESET signal). In the prototype set-up a mechanical switch has been used.

Table 1. Control signals for HDD and network card switches in the modified computer

HDD selection		HDD0 (data)			HDD1 (net)			net card	
HDD0	HDD1	CS0	CS1*	mode	CS0*	CS1	mode	CS	mode
-(SL)-	MR	1	0	OFF	1	0	ON	0	ON
MR	SL	0	1	ON	1	1	ON	1	OFF
MR	-(SL)-	0	1	ON	0	1	OFF	1	OFF

In Table 1 the logical states of the control signals CS0 and CS1 are presented. They make switching the computer to the modes shown in Fig. 1 possible. The SEL0 and SEL1 signals are produced by mechanical switch shown in Fig. 5b. Labels CS0 and CS0* (or CS1 and CS1*) show that switching of HDD disks is achieved by the use of inverse states for default logical level of the control line. This is possible by suitable setting of the SW, SW1 and SW2 connectors (Fig. 3).

5. A note about electronic parts of HDD and network card switches

Switches which are applied to break the DIOR, DIOW and INTRQ signals should be characterized by very short propagation time. The same applies to the breaker switch of the DEVSEL signal in the network card. In the prototype set-up fast NC7SZ384 switches from Fairchild Semiconductor were used [2]. Those devices are produced as SMD components with 0.25ns propagation time.

6. Conclusions

Hardware controlled method of data protection described above helps to increase the safety of files stored on the computer hard disk. The safety was achieved by physical cutting-off of transmission channels. The presented idea has been well verified; the experimental system has been working continuously for 2 years. During these years there was no necessity to regenerate the operating system located on the HDD0 disk. The HDD1 disk was designed to work under the network condition. During the same period the operating system installed on the HDD1 disk has been regenerated several times.

As it was mentioned above, the HDD0 disk was divided into two partitions. On the basic logical partition an operating system and processing software were placed. On the extended partition of the HDD0 the user data were stored. The separation between the system files and the data files simplifies the processes of

data and operating system archivization and recovering. The system recovery can be performed from the partition image made by e.g. NORTON GHOST software. In the prototype set-up the same operating system and programs have been stored on the HDD0 and HDD1 disks. In this way, the recovery processes of both partitions can be made from the same, single image.

HDD switches designed especially for this project demonstrated full effectiveness for the rate of information transfer in UDMA66 mode.

References

[1] Metzger P., *Anatomia PC,* HELION, Gliwice, (2001), in Polish.
[2] Data sheet: 'NC7SZ384 – TinyLogic™ UHS 1-Bit Low Power Bus Switch', Fairchild Semiconductor, (1999).
[3] Horton M., Mugge C., *Bezpieczeństwo sieci,* TRANSLATOR, Warszawa, (2004), in Polish.