Journal of Southeast University (English Edition) Vol. 21, No. 1, pp. 11 - 15 Mar. 2005 ISSN 1003—7985

Design and realization of security physical isolation system

Chen Youping[1] Yin Yong[1] Li Fangmin[2] Zhou Zude[2]

([1]School of Mechanical Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, China)
([2]School of Information Science and Engineering, Wuhan University of Science and Technology, Wuhan 430070, China)

Abstract: A physical isolation system based on PCI (peripheral component interconnect), embedded with intelligence card technology, strong identity authentication technology and security audit, etc., is introduced. The system can physically isolate the internal and external networks. The hardware of the system, including PCI interface control circuits, network interface circuits and logic control circuits, is designed to automatically adapt its operation speed and mode to the network and securely isolate the internal and external networks; the software of the system, including the security strategy management module, the security audit module, the database record exchanging module, the file exchanging module and the mail exchanging module, is designed to efficiently exchange and manage the data transference between the internal and external networks. Also the driver of the system is implemented with Windows driver development kits (DDK) based on Network Driver Interface Specification (NDIS). The prototype of the system developed has been employed in the Police Fire Protection Bureau of Hubei Province, which performs consistently and efficiently. The technological cruxes discussed have practical values for related subjects.

Key words: physical isolation; internal and external networks; PCI (peripheral component interconnect) bus; system management software; driver

Physical isolation is the ideal measure to utterly ensure network security. Many enterprises and government branches have been implementing physical isolation to safeguard their confidential data. According to the code in chapter 2 of the International Network Secrecy Management Norm of Computer Information System on January 1st, 2000, all the information systems involved in a nation's secrecy should be isolated physically from the Internet or other public networks[1].

Traditional security technologies, such as firewall, intrusion detection, encryption and so on, are based on software and implemented in logical mechanism, so they are vulnerable to attacks. Information security in networked manufacturing environment cannot be ensured. Physical isolation, a new protection technology in the information security field, which physically isolates the internal and external networks, can prevent private data of manufacturing enterprises from hacker's attacks over the Internet.

Through proof-test and application, physical isolation has been developing gradually since its birth. Till now, it has gone through three phases[2], and in each phase one type of typical special technology has emerged, namely double-computer network technology, double-hard disk isolation technology and single-hard disk isolation technology[3].

Nowadays about 20 companies are developing physical isolation products in China, and most of them are undertaking development or sale of products of the first or second phase[4]. A recent research on the application status of physical isolation indicated that the percentage of businesses requiring or applying physical isolation is less than 10%, which means physical isolation in our country is just beginning, and it needs to be studied extensively[5].

Furthermore, physical isolation, as a new booming security technology, is generally misunderstood by many people, which affects its application and development in China.

1) Physical isolation is not only studied and applied in China. Many reports show that this technology has been developing and applied in USA and Israel[6]. Prior to 1999, the US government said it was imperative that the confidential network of the military must be isolated from the Internet. Information about this technology in foreign countries is hardly reported because it relates to secrecy sensitivity and the security of the country, so related materials and reports are restricted.

Received 2004-06-23.

Foundation items: The National Aviation Creative Technology Foundation of China (No. 20000855), the Science Fund for Distinguished Young Scholars in Hunan Province (No. 03JJY1012).

Biography: Chen Youping (1957—), male, doctor, professor, ypchen@hust.edu.cn.

2) Physical isolation is merely a simple not a complex hardware scheme. This idea exists not only in the network security field, but also in China's IT field. Physical isolation, as other security projects, involves many aspects such as security strategies, security regulations, security management, etc.

3) Physical isolation simply disconnects the internal and external networks, compromising the aim of resource sharing over the Internet. Actually the purpose of implementing physical isolation is to be able to fully share resources over the Internet under the premise of network security.

Based on the analysis above, a perfect security physical isolation system based on PCI is introduced in this paper.

1 System Framework

As shown in Fig. 1, the framework is in the form of hierarchy, and its data-exchanging functional modules such as database record exchanging, file exchanging and mail exchanging, are provided with COMs, which offer the possibility to extend system functions. The system includes ten modules, in which the physical isolation card, the security strategy management module, security audit module and data exchanging module are kernel parts, and others are supplementary.

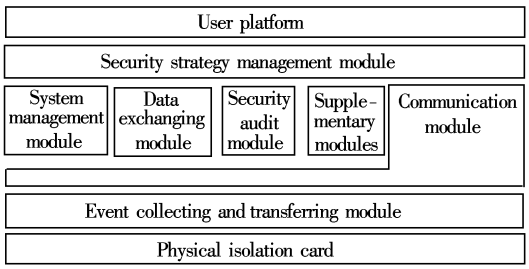

Fig. 1 Framework of the system

- **The physical isolation card** The card is the sole hardware of the system, which accepts control instructions from the management platform to connect the internal or external network, while disconnecting the external or internal network, and returns a report about operation status.
- **The user platform** The user platform is the interface between users and the system, through which the administrator can add, delete or configure system components.
- **Security strategy management module** Since this system is a barrier between the internal and external networks, its security level determines that of the internal network. Traditional user name and password are no longer satisfactory, and powerful identity authentication technology, cipher technology, digital certification, intelligence card and access control technology are embedded in the system.
- **Security audit module** The system can physically separate the internal and external networks, prevent the internal network from outside attacks, but it cannot ward off risks from the internal network. To implant a security audit module into the system can enhance the system's security level.
- **System and component management modules** System and component management modules are the interface to configure the system and COM, through which the administrator can set up their attributes.
- **Data exchanging modules** Currently the system contains three data exchanging modules, namely the database record exchanging module, file exchanging module and mail exchanging module, which are kernels of the system, and all data exchanging between the internal and external networks depends on them. Different threads are forked according to different business requirements, and these threads can work together or independently.
- **Event collecting and transferring module** This module is the bridge between the user platform and the physical isolation card. It sends instructions to the card and checks feedback from it. Also, this module monitors requirements from the system, and sends them directly out or puts them into the message queue according to the current status of the system.
- **Supplementary modules** These modules provide wizard or help files for the system.

2 Hardware Design and Realization

The physical isolation card works on a common server connecting internal and external networks, and it changes the connection status depending on the switching instructions from the user management platform. The card integrates the function of a 10 M/100 M adaptable network card, serving as two network adaptors and one physical isolation card. The card can also distinguish the transferring speed and the mode of the switcher or the hub connecting to it, and automatically adjust its own speed and mode. The framework of the hardware is shown in Fig. 2.

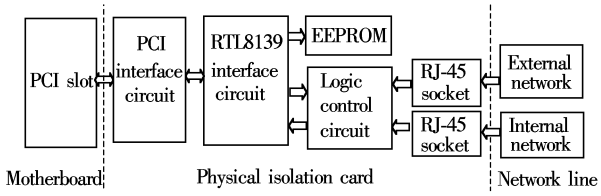

Fig. 2 Framework of the hardware

The design idea of the card is as follows:

1) The computer will load the driver of the card when the system starts, and it connects the internal network in default, while disconnecting the external network. The card can be configured to work in the internal network status automatically.

2) When the card receives switching instructions, it performs a series of operations such as disconnecting the internal network while connecting the external network. As the configuration parameters of the internal and external networks are partly different, the attribute parameters of the card will be set as an external network status through a registry table.

3) The switching operations can be handled through clicking the button on the user management interface, and they can also be performed automatically through presetting operation rules.

Fig. 2 shows the structure of the card's hardware, which is composed of a PCI interface circuit, RTL8139 chip interface circuit, configuration EEPROM, switching logic control circuit and RJ-45 sockets, etc. The card should be inserted into the PCI slot of the motherboard, and the internal and external network line should be inserted into the RJ-45 sockets.

In a normal case, the card works as a common network adaptor. When it works in network exchanging mode, the system sends out control instructions, and through the PCI interface of the motherboard, under the control of the PCI interface circuit and the RTL8139 chip interface circuit of the card, the instructions reach the switching logic control circuit to execute the network exchange.

3 Software Design and Realization

The physical isolation system is an integrated scheme for network security, including the software and the hardware. The software of the system is composed of the system management module and the driver for the card.

In the system, the card is based on PCI interface, controlled by instructions from user management platform. The driver links the card and the user management platform through the DLL module, namely the DLL module is the median unit between the user application and the driver of the card, as shown in Fig. 3. When the card works, the user management platform sends out exchanging instructions through the DLL module to change the network status.

3.1 System management software design and realization

The system management software contains a security strategy management module, security audit module, database record exchanging module, file exchanging module, and mail exchanging module, etc, which are introduced as follows.

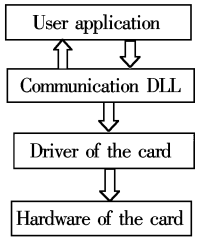

Fig. 3 Interface between the card and user application

3.1.1 Security strategy management module

This module is composed of an identity authentication unit and role-based access control unit, and its core technology mainly includes digital certification, cipher technology, an intelligence card and role-based access control technology. A certification authority — a validity authentication center, which is responsible for digital certification issuing, checking, deleting, and so on — issues digital certification[7]. In this system, certification of the X509 format is adopted, the private key of which is stored in an intelligence card, and it can only be accessed with the correct password. The workflow to access the system with an intelligence card is shown in Fig. 4. Users are required to insert the intelligence card into the card-reading machine when they access the system. The information on the digital certification will read out, and the subject and serial number of which will be abstracted with GetInformation and GetSubject functions. Then the system will compare the subject and serial number with those stored in the database. If they match, the system will start up; otherwise users cannot access the system, and the system will record any unsuccessful access for later audit.

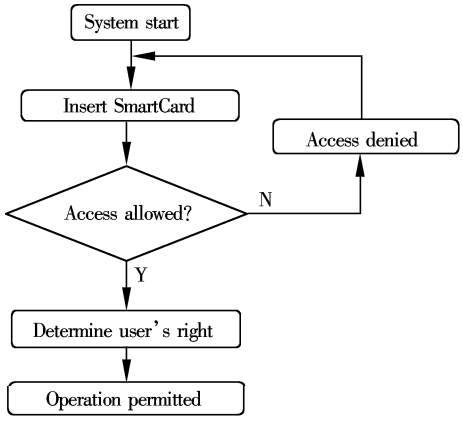

Fig. 4 Workflow to access the system

3.1.2 Security audit module

The system can not only separate the internal and external networks, but also partly substitute firewall by adopting security audit module to enhance its security robustness. The framework of the security audit module is shown in Fig. 5. Items for audit are from three sources, namely: ① abnormal events from the operating system that are possibly induced by itself or outside intrusion, ② abnormal events from the physical isolation system that are possibly induced by incorrect operation of it or malicious operations of an illegaluser, ③ intrusion from the Internet. As for these abnormal events, the system can choose corresponding disposal according to the source type. For urgent events such as intrusion of a wood horse or system breakdown, the expert unit will send reports to the alarm unit, and the alarm unit will give out different alert signals according to different event content. Currently three types of alert signals are designed in the system. One is sound alert by a speaker, one is BP alert to BP machine, and the third is message alert like OICQ or MSN. For common events such as failure on system start, abnormal service and so on, the audit operation can be delayed or ignored.

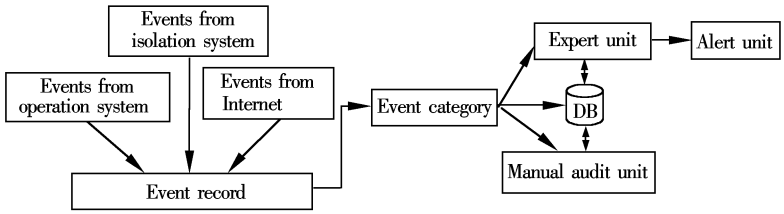

Fig. 5 Structure of security audit module

3.1.3 Database record exchanging module

The database record exchanging module is designed for data exchanging between databases in internal and external networks. In this system, SQL Server database and Access database are designed, but other types of databases can be added into the system as extended modules according to user's requirement. The system can automatically configure database resources in database attribute dialog of the user management platform, so that there is no need to configure ODBC in the control panel. The system will delete the database resource automatically after transferring data.

3.1.4 File exchanging module

The file exchanging module transfers file data between the internal and external networks with FTP. To transfer data efficiently, the system utilizes parallel transferring technology, that is, the platform can send and receive data at the same time. Also a matrix variable is defined to store information about the file. In the configuration file of the file-transferring component, the file and its directory are configured. If the same name of the file or directory is found, the system will inform the user to overwrite or skip it.

3.1.5 Mail exchanging module

In the mail exchanging module, ESMTP and POP3 are utilized as a bridge to exchange mail data between the internal and external networks. To realize mail data exchanging, the system provides clients for mail sending and receiving. When the system connects with the external network, the client communicates with the mail server on the external network, downloads mail from the outside, while sending mail to the internal server. Correspondingly, when the system connects with the internal network, the client communications with the mail server on the internal network, sends mail to the internal server, while putting mail from the internal network outside. Since only clients of sending or receiving mail are designated in the system, the third mail server is needed when mail is being transferred.

3.2 Driver design and realization

In the Windows operation system, especially in Windows 2000 and Windows XP, to ensure the security and generality of the operation system, the access of application programs to the hardware resources of the computer is restricted, that is, no application programs can directly access the hardware of the computer, so the driver of the card in the system is necessary. Since Windows 2000 is the most popular operation system nowadays, the driver of the card is designed based on the Windows driver module (WDM).

Microsoft and 3COM have been advocating Network Driver Interface Specification (NDIS), which provide a standard program interface for general and universal network-related driver design[8] on the X86 platform. To design drivers with NDIS, we only need to call NDIS functions, and it is not necessary to consider the kernel of the operation system and the interface of other drivers. The driver of the physical isolation card in the system is developed based on NDIS, and in fact it is a mini-port network driver, which includes two functions: ① The driver should control the card to send or receive switching instructions; ② The driver should have an interface with upper drivers such as the median layer function drivers and other transfer drivers. The mini-port driver communicates

with the card and upper drivers through NDIS library. NDIS provides a whole series of functions whose names begin with NdisXXX. These functions encapsulate all interface routines for the driver. Moreover, the mini-port driver provides a suite of entry functions, namely MiniportXXX functions, so that the NDIS can access the mini-port driver[9]. During data transferring, the mini-port driver communicates with the NDIS and other upper network protocol drivers.

4 Conclusion

Physical isolation is a brand-new security strategy developed in recent years, which meets the security requirement of confidential information for many units. With the development of this technology, it is becoming an indispensable component of information security. The system presented in this paper not only physically isolates the internal network from the outside, but also embeds many other security technologies such as an intelligence card, identity authentication, cipher technology and so on with many business applications, which provide a perfect security scheme for high level secrecy. The prototype of the system developed in this paper has been employed in the Police Fire Protection Bureau of Hubei Province, performed consistently and efficiently. It meets the requirement that the internal network must communicate with the Internet but also be physically isolated from the Internet.

References

[1] Wei Si Company. Several key points in deploying physical isolation technology in confidential network [J]. *Secrecy Works*, 2002, **7**(5): 34 - 35. (in Chinese)

[2] Zhao Zheliang, Huang Qingfang. Several understandings about network physical isolation [J]. *Technology and Application of Network Security*, 2002, **4**(2): 14 - 16. (in Chinese)

[3] Wu Gan. The current status and development of physical isolation technology [EB/OL]. Http://www.ccw.ccw.com.cn/htm/net/seminar/01_8_31_2.asp. 2003/2004-04. (in Chinese)

[4] Wei Wei. The development trend of network security [EB/OL]. Http://www.ict.ac.cn/inf/safety.htm. 2003/2004-03. (in Chinese)

[5] Li Haiming, Li Zhipeng. Analysis on physical isolation technology of Chinese [J]. *Network World*, 2002(3): 30. (in Chinese)

[6] Northcutt S, Zeltzer L, Winters S, et al. *Inside network perimeter security* [M]. New Riders, 2003.4.

[7] Carlisle A, Steve L. *Understanding public key infrastructure: concepts, standards, and deployment considerations* [M]. Indiana: Macmillan Technical Publishing, 1999.

[8] Yi Fasheng, Peng Mei. The structure of Windows and the design of network driver [J]. *Computer Application*, 1999, **11**(10): 61 - 63. (in Chinese)

[9] Cant C. *Introduction to design of WDM device driver* [M]. Translated by Ma Li. Beijing: China Machine Press, 2000. (in Chinese)

一种安全物理隔离系统的设计与实现

陈幼平[1] 尹 勇[1] 李方敏[2] 周祖德[2]

([1] 华中科技大学机械科学与工程学院, 武汉 430074)

([2] 武汉科技大学信息科学与工程学院, 武汉 430070)

摘要: 提出了一种基于 PCI 总线的物理隔离系统, 该系统采用物理隔离技术、强身份认证技术、安全审计技术等实现内外网的物理隔离. 利用 PCI 接口控制电路、网络接口电路和逻辑控制电路实现了系统的自适应网络功能和内外网的安全物理隔离, 能自动识别所连接网络设备的速率和工作方式, 并自动将工作方式和速率调整到正确的模式与之相适应. 系统管理软件包括安全策略管理模块、安全审计模块、数据库记录交换模块、文件交换模块和邮件交换模块, 以实现内外网数据安全高效的交换和管理; 使用 Windows DDK 实现了基于 NDIS 的硬件驱动程序. 系统原型已在湖北省公安消防总队政府上网工程中稳定高效地运行, 其关键技术的实现对相关课题研究具有普遍意义.

关键词: 物理隔离; 内外网; PCI 总线; 系统管理软件; 驱动程序

中图分类号: TP393.4