Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(1):62-66

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

Design and enforcement of a safety information system in E-Bank

Yanli Liang

Henan Institute of Science and Technology, Xinxiang, Henan, China

---

ABSTRACT

Internet banking is an extension for the private internet of present banking as well as a supplement for business structure of traditional banking and with the increase of some software as well as hardware instruments, users can connect the banking system with home computers to process some common banking business, which remedies the deficiency of operating branches as well as operating time for traditional banking business. To realize adopting fire wall on network layers which prevent extraneous attack and guarantee the safety for business data transportation on the public internet, integrity identification as well as key management should be simultaneously implemented on the application layers for sensitive data as well as encrypted information. In the context of the safety for internal banking business system as well as the safety for external banking business, this project preceded the internet safety design from the aspects of various banking business, business connection between the head office and branches, OA system and internet banking. In this project, high-quality fire walls are equipped on the panel points of all subsidiary banks of different levels, which guarantee the confidentiality of the IP package. Meanwhile, users' sensitive information can be protected in business system form illegally distorted, which will achieve the safety functions of encryption as well as identification for business data.

Key words: Implementation, Safety Information System, Electronic Banking

---

INTRODUCTION

With the large-scale popularization of the internet, each bank has been progressively developing its own internet banking system. The promotion of internet banking operation has critical significance of reducing coast as well as increasing efficiency and simultaneously brings about safety threatens, which tremendously confines the further generalization of internet banking operation. In recent years, a vast cases of internet banking defrauds have been reported. Criminals filch users' ID number as well as password to steal or falsely use large quantity of money [1]. Regardless of many advantages in the internet banking for banks as well as users and under this situation, the promotion of internet banking will encounter tremendous risks, and the security of internet banking should be enhanced immediately [2]. According to the analysis of common reports, criminals mostly use the Trojan virus to filch users' information, for example hackers firstly transfuse the Trojan program into users' computer system, and the monitoring system remains in the target computers can intercept and monitor the system as well as the internet banking password window when users are surfing the internet. In other words, when users are inputting the ID number or password in the internet banking system, the computer will automatically deliver the code of relevant information to the hackers, which can be reversely read as well as decoded, and in this way money is carried away by the hackers [3].

Information network technology application is increasingly popular and widely, such as Internet, application fields transfer from the traditional small business system gradually to large key business system extension, typical of the party and government departments such as information systems, and financial service system, the enterprise business system, etc [4]. Network security has become an important problem affect network performance, and the Internet is open, international and freedom in increase the application degree of freedom at the same time, the

security put forward higher request, this mainly displays in: open network, leading to the network technology is full open, any one person, group could get, so network faces destruction and attack may be various [5]; Network attack not only from the local network users, it can come from the Internet and a machine; Liberty means the network user's use and did not provide any technical constraints, the user can freely access to the network, free to use and distribute various types of information [6].

In a word, open, free, and the internationalization of the development of the Internet to government agencies [7], enterprises and institutions has brought the revolutionary reform and opening up, make they can use Internet to improve work efficiency and market reaction ability, in order to become more competitive. Through the Internet, they can retrieve the important data from other places, at the same time, to face the open Internet bring data safe new challenges and new risk. Based on this kind of situation, considering the complexity of the application system, to establish the system of network security and network security and comprehensive solution is imminent.

ANALYSIS OF THE HIDDEN DANGER OF BANK ON THE NET

The net system's main problem is that the user security too dependent on the quality of the user itself, for safety concept poor user, the password is easy to being stolen, so the "trust users" safe mode design is not reasonable. The user's computer may install Trojans, user actions are likely to be monitored and steal, safe net system should be designed as such: suppose net administrator is hackers, and in the end user computer installation Trojan and can monitor the user's all keyboard mouse operation net silver, the administrator can also for system management and operation, but net administrator is still unable to through the net system to steal the money end users. If you can do this, then the net system is a relatively safe [8].

Computers controlled by hackers: If a computer hacker’s successful control for "chicken. so when the user use the computer for online banking operation, hackers may monitor to the relevant online banking operation action, and use the Trojans get account password, and by using the users are using the U shield and mobile hardware number certificate, success will are using online bank transfer. This is the premise of possible, first is causes by remote computer control, second it is the users are using U shield for Internet bank transfer, and third is the user didn't use cell phone verification and other services.

The risk of IE browser being hijacked: U shield is the function of trading information to encrypt the authentication; the authentication of trading information can meet the accurate and complete, and shall not forge undeniable characteristics. In the actual net operation process, users in the IE browser form trading information, again by IE browser the transaction information to the U shield for the authentication. U shield fully trust the IE browser, even if IE submitted a pen after tamper with the deal, U aegis also cannot find, so for the authentication. Therefore, if a Trojan virus through some technical means, able to take full control of the IE browser, can to net user's transaction information manipulation, once the user the confirmation, the business is tampered and normal trade, after the authentication, send, and ultimately perform.

False online trading orders: The virus in the monitor to the computer users in online shopping, will take the user's current page jump to hackers special set false payment page. Because of the online shopping but are generally the same home third-party payment platform (such as clap nets of payee is Shenzhen ten cent technology company, taboo’s payee is Zhejiang pay treasure network co., LTD., etc.), true and false web pages with only order number and transaction amount of difference, this situation often have careless users click confirm payment, the result that normal shopping money to pay for hackers in the bogus account [9].

Loopholes in the third party payment platform: Many online banks and the third party trading platform on the butt, this will give hackers steal the user of the bank on the net capital provides in machine. The third party trading platform had been can be use of loopholes, and happen too much money on user stolen case. Because the bank on the net and the third party trading platform are closely related, therefore the safety of third party trading platform for the development of the bank on the net effect also knots allow to ignore.

THE PRINCIPLE OF DESIGN AND REALIZATION OF THE BANK ON THE NET SECURITY SYSTEM

A security defense system is usually to achieve the objective: to prevent outside hacker attacks; To prevent from the inside of the malicious attacks; Network resource access control; Network transmission of real-time monitoring; Strong safety audit mechanism; Event analysis and warning measures, etc. In order to achieve the above purpose, usually by in the network layer on the firewall to prevent foreign attack and guarantee business data in the public network safe transmission, at the same time in the application layer to provide a sensitive data encryption message integrity identification and key management. This program will from various business bank, bank head office and branch business links and OA system, the bank on the net all aspects of network security design. Design in the various branch node equipped with high performance firewall to ensure confidentiality of IP packet, and at the same

time in the business system to protect the user sensitive information, prevent information is illegal manipulation, realize the business data encryption, identity authentication and so on security function. Therefore, in the bank all an export configure the firewall, the head office and branch of the joint network, also configuration firewall, foreign prevent hackers, internally to prevent internal personnel's malicious attack or due to internal personnel caused by the problem of network security [10].

DESIGN OF BUSINESS AND OFFICE SYSTEM SAFETY

In the bank business system security design, mainly involves are the bank head office and branch network interconnection and bank internal office operation system. Security measures are:

Business system isolation: On the network bank to various applications, including RMB business system, foreign currency business system, internal OA system and a series of business, the business is a link between, to guard against infringement use resources, especially the banking system and office OA system, the operation system is the guarantee of the isolation system security industry an important link. In the bank's internal, each business systems use host IP address is strictly distinguish, to build access control mechanism is the core of the isolation measures provide convenience. Points head office, branch and branch between, through the VLAN division, business VLAN and OA VLAN, isolation office network and network, can isolate business VLAN and OA VLAN as needed to realize communication.

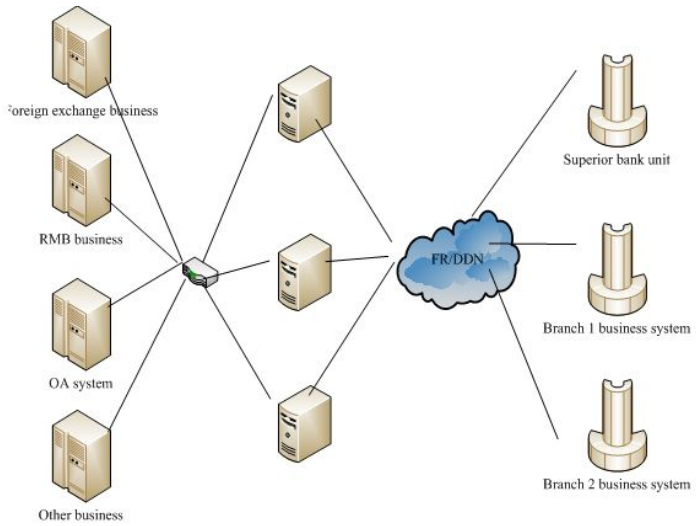

Fig.1.The bank system business isolation scheme

The protection of sensitive data: In the banking system there are many sensitive data area (such as the banking system host, etc.), these sensitive data area requirements strictly confidential, to access permissions have strict restrictions. But the bank system all the host in the same network system inside, if not controlled, it is easy to cause the network and network within the malicious attacks, so in these data area entrances will be strictly controlled, so in these places configuration firewall, as shown in Fig.2 shows.

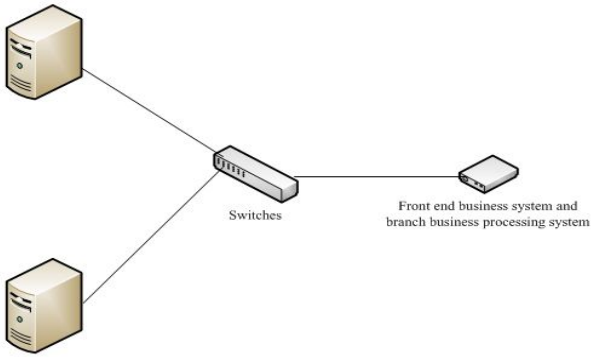

Fig.2.Sensitive data area protection scheme

The firewall performs the following control functions: to visit packet filtering, the only allowed verify lawful host packets through the ban all unauthorized host access; to visit the user verification, to prevent illegal user's intrusion. Using network address translation and application agent make data storage area and business front host isolation, business front host does not directly and data storage area to establish the network connection, all of the data access

through the firewall application agency completed, to ensure the safety of data storage area.

Data encryption: In the bank's wan transmission system, from the head office to branch, the branch to branch, branch to a small local branch and so on, these line most are made by public sector communications company provide, and many users in a system to carry out their business. Because these lines at the same time exposed to the public, it is apt to cause the data stolen. So for data transmission encryption is a very important link. In this method, the headquarters to each branch, and branch to branch using VPN encryption technology for data encryption. Implement all of the VPN products can realize communication. In the system, and use VPN technology to encrypt data transmission way as shown in Fig.3.

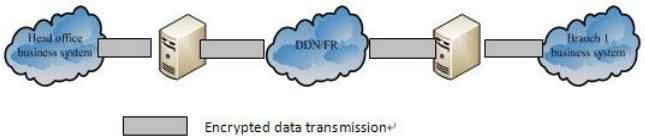

Fig.3. Use VPN technology to encrypt data transmission

Firewall for protection: To ensure the security of the network, firewall must protect itself to ensure safety. System power supply, hardware fault and other special situation occurs, will make the firewall system paralysis, and seriously hinder the network communication, so the requirement firewall has redundancy protection measures and enough ability to attack. Here the firewall dual-machine backup plans, as shown in Fig.4:

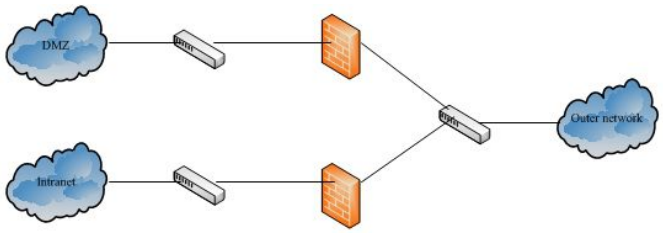

Fig.4.Firewall dual-machine backup plan

DESIGN OF ONLINE BUSINESS SAFETY

In this scheme, we combined with online banking system structure and its facing the problem of network security, adopt the following safety measures: in bank electronic commercial platform and Internet outlet installed Net Screen - 100 firewall; The Net screen - 100 virtual IP technology, electronic commerce server do load balance; In the bank and bank comprehensive e-commerce platform between network installation Net Screen - 100 firewall; Enable Net screen - 100 VPN channel function, using the standard encryption technology to transfer data encryption. In the bank electronic commercial platform and Internet installed Net Screen between 100 -, -, through its based on state detection of packet filter, can effectively will be illegal packet out outside the firewall; Through the NAT (network address translation) will internal server (such as providing e-commerce services server) IP address into external IP address, can effectively prevent hackers from through various means to attack or invasion of internal server, in order to ensure that the electronic commercial platform from invasion, and all the information blockade, and open in hope to provide services.

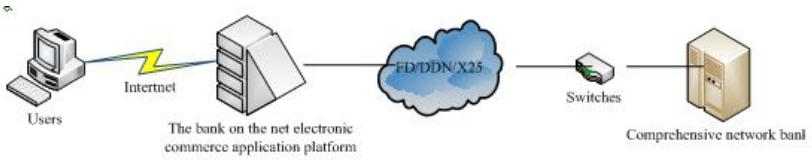

Fig.5.The bank on the net security system design

CONCLUSION

In this project, NetScreen-100 is adopted as fire wall on connections between head office and subsidiary banks, and simultaneously the particular multi-machine backup technology of Net Screen is applied on the important business connections, which guarantee the internet safety for the entire system with two machines as hot back up. The safety

system construction of the internet banking application system is an extraordinary complicated systematical engineering, which requires programming in advance as well as deliberate choice. In most situations, various safety technologies as well as management should be integrated to achieve it. The safety for hardware instruments as well as system platform can be enhanced or preceded by multiple technologies. It is reminded that many safety threatens derive from management deficiency as well as cognition for safety threatens, especially the vulnerable safety awareness of the users as well as the management system vulnerability. A favorable safety management contributes to enhancing security of the system, which includes finding safety vulnerabilities of the system in time, investigating the safety system, enhancing the education of safety knowledge for users and establishing a complete management institution of the system.

REFERENCES

[1]Fan ChangXing, Wu Qiang, Shao QingJing. *IJACT: International Journal of Advancements in Computing Technology*, **2012**, 4(21), 405-413.
[2]Chen Qiaoping. *AISS: Advances in Information Sciences and Service Sciences*, **2012**, 4(16), 14-22.
[3]Dong Yang, Lei Liu. *AISS: Advances in Information Sciences and Service Sciences*, **2012**, 4(21), 63-71.
[4]Hao Yanling, Mu Hongwei, Jia Heming. *AISS: Advances in Information Sciences and Service Sciences*, **2012**, 4(21), 598-605.
[5]Guo Jintao, Xin Jiang. *IJACT: International Journal of Advancements in Computing Technology*, **2012**, 4(21), 76-83.
[6]Horst Lichter. *JDCTA: International Journal of Digital Content Technology and its Applications*, **2012**, 6(21), 11-15.
[7]Miao Naiming. *AISS: Advances in Information Sciences and Service Sciences*, **2012**, 4(21), 99-105.
[8]Li Shi, Hong-bin Dong. *JDCTA: International Journal of Digital Content Technology and its Applications*, **2012**, 6(16), 112-119.
[9]Yu A-Long. *IJACT: International Journal of Advancements in Computing Technology*, **2012**, 4(21), 574-581.
[10]Zhang B.. *Int. J. Appl. Math. Stat.*, **2013**, 44(14), 422-430.