

Study on Security Problem and Its Strategy of Computer Network in Bank

ZHU Zhenfang

School of Information Science and Electric Engineering
Shandong Jiaotong University, Jinan, China
zhuzhfyt@163.com

Abstract: *The bank of the computer network security is the very concrete reflection of computer security in financial industry. Computer network technology which is fast developing has raised the bank's work efficiency, service quality and management level. It is beneficial to satisfying bigger social demand. However, computer network technology also makes bank computer network security issues frequently. There is more and more threat to network security. The main research direction of this paper was Computer Network and Application Technology which was fast gaining popularity in the banking industry, put forward how to solve the computer network security problems in banking industry so as to provide valuable information that coping with bank computer network security construction.*

Keywords: *Bank Computer, Network Security, Network Security Technology, PPDRR security model.*

1. INTRODUCTION

Since the reform and opening up, the economy in China develops rapidly and healthily, and the financial market is more open and globalization accelerates after China entered into World Trade Organization. As the main component of Chinese economic entity, the competition of banking industry becomes more violent. In order to pursue the maximum profit, banks innovation technology competitively and pay attention to emerging network banking market. With the rapid development of information, many banks start various internet-based banking services successively based on computer network system. Because of the resource sharing property, computer network system greatly improves the efficiencies of business handling. However, all of these characteristics of computer network also increases the possibility of being attacked while brings new hope to banking industry. Therefore, all the banks should ensure the high security of computer network system to stand firm in fierce competition.

2. COMPUTER NETWORK SECURITY IN BANKING INDUSTRY

In China, with the wide application of computer, the application of computer network for banking gradually develops to internet which makes computer network become an important direction of the computer application in banking. However, the computer network for banking provides convenience to users, but also gives opportunities to do destructive activities against the implementation of computer network system because of the euroky of distribution, openness of network system organization, sharing of network resources, and the commonality of network information [3]. Once upon the computer network system in bank have problems, economic chaos and paralysis may occur in a department, region, or even a country. Banking is closely related to the economic lifeline of the country, so the computer network security of banking is one of the important subjects for computer network security, while the computer network security of banking is the key to ensure banking business in order, maintain the country and society stable, and produce social benefit.

3. COMPUTER NETWORK SECURITY OF BANKING

3.1. Defects of Computer Network Technology for Banking

In general, the customer group of bank comes from all over the country, so the computer network for banking is featured with wide geological scope, large customer group, high resource sharing degree, and great information value. Therefore, the threats and attacks faced by the network system for

banking increase and become more complex. In addition, the computer network system for banking always uses internationally-used TCP/IP protocol which may cause interception, cryptanalysis, and tamper of important information (i.e. customer code, account, contact, etc.) during transfer in Internet. Moreover, as the center of financial system, bank network cannot avoid the security risks from internet, external connection, and internal network because of its large sale of network construction and great connection points [5].

3.2. Defects of Computer Software

The problem of computer network security for banking is always resulted from the defects of system in logic design. Illegal person always does destructive activities (i.e. virus implantation or Trojan horses) by making use of error or defect of application software in computer system through network to make user's computer fall into paralysis or be controlled by intruder. Meanwhile, hackers can steal important data and information after controlling the computer by the loophole in computer operation system. This will take disadvantageous effects on users [6].

3.3. Defect of Computer Hardware

The communication by any way requires pass through processor, convertor, modulator, network port, line, and other fundamental components. All of these components are the hardware equipment of computer which constitutes the channel of data transfer between users and foundation for all communications. However, the objective problem is that these fundamental components are exposed outside and will cause signal radiation for non-strict shield or non-shield to become the target of stealers and attackers. The communication system of computer network for banking is also based on these fundamental components, so the defect of computer hardware is also the disadvantageous factor to threat the security of computer network system for banking.

3.4. Hackers and Virus Attack

Bank is the center of financial market, so hackers prefer to attack the computer network system for banking driven by benefits. In the open network platform, hackers conduct malicious damage to computer network based on the exquisite computer technology. The forms of threats against banking computer network security by hackers include eavesdrop, illegal terminal, illegal intrusion, and computer virus.

3.5. Poor Network Management in Security Management System

Banks have not established improved standard security management system for information system with insufficient security management strength. The implementation of management strategy is lack of exchange and communication channel, while some real-time security problems are lack of proper feedback and solution method; banking security management organizations or technical institutions are lack of professional talents of security technology. Moreover, because of the lack of effective cultivation shaping in consciousness of security protection, banking employees always step in and take the advantage by stealing banking secrets with weak self-restraint to cause internal stealing from banking network.

4. SOLUTIONS TO COMPUTER NETWORK SECURITY FOR BANKING

4.1. Construction of Security System Framework

Enhanced encryption technology is used to encrypt data, develop secret key system, data integrity, and digital signature standardization, and construct the safety system framework connected with open system. The security control guidance to computer system for banking is proposed based on the threat analysis and vulnerability analysis, and various security limits are supplied. With virtual net technology, the whole computer network is divided into several independent subnets [9] according to different applicant demands to describe all the security services, mechanism, and management to set foundation to construct a safe and open computer network.

4.2. Security Arrangement for Administrative System

- For bank employees, especially staff involving confidential data should be educated in security and secrecy to make them strictly follow operation procedures and secrecy plans and avoid accidents, such as manual stealing and damage and virus.

- Establish safe and qualified machine rooms and mechanism for processor of banking computer network system and all terminals; set close shield room; prevent criminal offender with public security, safeguard, etc.; construct facilities for fireproofing, disaster prevention, and other accidents; set measures to avoid damage of storage equipment for power failure; and set other emergency and backup measures and crypto security measures to prevent illegal users from intruding through line.

4.3. Security Measures for Physical Equipment

Take various protection measures to prevent transmission line from being interfered by radiation and reduce data transmission error; place the concentrator and modem under monitoring and take regular inspection for connection to prevent external attempt and detection from being tampered; strictly custody the storage media with data, such as hardware and discs to prevent stealing, reproduction, and damage, and take strict encryption when writing data into storage equipment to ensure that only users with secret key can use the stored data information.

4.4. Security Measures for Information Protection

In order to prevent illegal intrusion and information stealing, following security technologies are always used:

- Data security encryption, such as link encryption, node encryption, and end-to-end encryption in data network;
- Security technology for qualification inspection, such as call-back protection, command and digital certificate, access right, access control, etc.;
- Suppression technique for electromagnetic leakage, such as shield cable, metal shield room, and optical cable transmission;
- Record behavior of illegal users. When user behavior does not conform to record information, it should be determined that the computer network for banking is illegally intruded. There are two methods to judge if user behavior is legal, including separate method and continuous method [10].

5. CONCLUSIONS

In order to solve the security problem of data information in computer network for banking for open system organization, various threat factors, and wide application field to ensure stable development of computer network security, people who construct the public security system for computer system should make analysis according to international information security standards proposed by international organizations, such as ISO, IEC, and NIST. Therefore, the security target for computer network system construction can be obtained and security measures with integrity, coordination, and effectiveness can be set to play an important role in banking computer network security.

ACKNOWLEDGMENTS

National Natural Science Foundation (61373148), National Social Science Fund (12BXW040); Shandong Province Natural Science Foundation (ZR2012FM038, ZR2011FM030); Shandong Province Outstanding Young Scientist Award Fund (BS2013DX033), Science Foundation of Ministry of Education of China (14YJC860042).

REFERENCES

- [1] Baidu computer network [EB/OL]. <http://baike.baidu.com/subview/25482/6491244.htm>. Encyclopedia.
- [2] Yuan Jianfeng. Computer network security issues and preventive measures [J]. China scientific and technological information, 2006 (15): 150-157.
- [3] Zhu Ying Lin, Gou Zhaopin. Facing the computer network security problems and countermeasures [J]. Guizhou University Journal (NATURAL SCIENCE EDITION), 1993, 10 (4) 227-233.
- [4] Xie Xiren. Computer network (Fifth Edition) [M]. Beijing: Electronic Industry Press, 2012
- [5] Zhang, Wei Hongqin. Bank computer network security construction of [J]. Science and technology information, 2006 (8): 248-249.

- [6] Li Peng. On the computer network security issues and treatment measures [J]. times education, 2013 (5): 150
- [7] Baidu <http://baike.baidu.com/link?url=vFBsZXczn4gV7e073eLrKMe4> [EB/OL]? 2TLzLpjJT sRBw7X6qHBrWwFjhKAyE9juaAiS8pdCPxIWAcXzN-GAmW2lrkTXK.
- [8] Zou Zhanbo. Research and application of digital signature technology in the electronic government affairs [D]. Dalian: Dalian University of Technology, 2005
- [9] Wang Jimei, the gold Lianfu. Web service security strategy research and application of [J]. Computer applications and software, 2006, 21 (2): 91-93.
- [10] Sun Nan, Jiang Mountains. Research on security of bank computer network system [J]. Journal of Liaoning University (NATURAL SCIENCE EDITION), 2000, 27 (4): 329-332.
- [11] (US) Andress. Mandy computer security principle, [M]. Yang Tao, Li Ming., Beijing: Machinery Industry Press, 2001

AUTHOR'S BIOGRAPHY



ZHU Zhenfang, PhD, lecturer, he was born in 1980, Linyi City, Shandong Province. He obtained Ph.D. in management engineering and industrial engineering at the Shandong Normal University in 2012, his main research fields including the security of network information, network information filtering, information processing etc. The authors present the lecturer at the Shandong Jiaotong University, published more than 30 papers over the year.