Computer and Information Science
www.ccsenet.org/journal.html
Vol. 2, No. 3
August 2009

Analysis of Network Security and Risks Prevention Strategies of Hongqiao Airport West Terminal

Chongjun Fan (Corresponding author)
Business School, University of Shanghai for Science and Technology
Shanghai 200093, China
E-mail: cjfan@sh163.net

Honglin Xiong
Business School, University of Shanghai for Science and Technology
Shanghai 200093, China
E-mail: dianyi0467@yahoo.com.cn

Haiying Zhang
Shanghai Airport Construction Headquarters
Shanghai 201202, China

Wujun Liu
Shanghai Airport Construction Headquarters
Shanghai 201202, China

Liqiang Wang
Shanghai Airport Construction Headquarters
Shanghai 201202, China

Xiaohui Song
Shanghai Airport Construction Headquarters
Shanghai 201202, China

The research is financed by the research project of Science and Technology Commission of Shanghai Municipality of China. No. 06211212051 (Sponsoring information)

Abstract

The sharing and openness of network are convenient to the airport operations and passenger information inquiry, but also result in information security issues. In the design of Hongqiao Airport West Terminal network system, information security issues have been taken as important topics, and preventive strategies which aim at the specific circumstances have been formulated by comprehensive analyzing the causes of potential security hazard of airport network system security. This project can provide reference and help to related Chinese airport's planning and construction projects.

Keywords: Airport information system, Network security, Risk prevention

1. Introduction

With the accelerated pace of life, convenient flights information is a prerequisite for people on easy travel, which requires the airport network system to access internet stably and to provide open, timely, relevant and reliable information. Airport network system is the communications infrastructure for the whole airport information system and it supports the business operations on internet by connecting a wide range of interfaces to the various related system.

Based on the principle of "unified planning, phased construction”, Hongqiao Airport West Terminal network system has used leading mature and reliable technology to built Hongqiao wet terminal main network, west terminal wireless network, West Terminal POS network, the West Terminal security network system, west terminal internal communication system, which provide the 24-hour continuously reliable and safty data and media operating platform for information system. This platform is required to support the operation of Hongqiao Airport and to supply timely, accurate, systematic and comprehensive flight information services to the passengers, airlines, Hongqiao integrated transport public information platform and the business management.

In order to optimize manufacturing operations and equipment running, the platform is also demanded to help each airport departments to conduct multi-airport, multi-terminal scheduling management under the command of AOC/TOC (Airport Operation Center, Terminal Operation Center) agreement.

Hongqiao Airport is an important aspect in the Hongqiao comprehensive transportation hub projects. And these projects extend to outer ring in the east, Huaxiang Road in the west, Beizai Road in the north, Luqingping Road in the south. The completed airport will be 5.8 times as big as present scale. Such a large project can not be separated from the complex network system and the network system is the priority among priorities, because a security and reliable network is the core link of the whole projects.

2. The Planning and Designing Of Hongqiao West Terminal Network

2.1 the main planning and designing of West terminal network

2.1.1 the main planning of West terminal network

As main network, the joint room of West terminal network AOC, TOC is the core node for the entire airport's network the MDF-1 and MDF-2 are the main aggregation nodes, the MDF-3 and MDF-4 are node cluster when the West Gallery is enlarged in the long term. Core nodes and aggregation node are connected by using stars model. Set aside the network interface with the East Terminal. In the future West Terminal AOC will connect with the Pudong AOC remotly in order to make the two airports share information and resources for effective allocation and scheduling. It is shown in Figure 1.

(1) Pudong Airport connection. Between Hongqiao Airport AOC and Pudong Airport AOC a dedicated network interface is established which is optical fiber-based links and the telecommunications backup line is reserved. The network interface can provide two integrated systems, flight tracking system and within system which were interoperability required.

(2) Interface with Hongqiao integrated transport hub public information platform. Through the airport security isolation equipment the network share information platform interface with hub, and use the public flight information server to provide dynamic information-sharing platform for flight information.

2.1.2 The design of the core Main-net of West terminal

The core Main-net of Western Terminal is shown in Figure 2. The Western Terminal’s AOC/TOC joint machine room act as the data center and main-net center, the Main Distribution Frame MDF-1, MDF-2 in gallery Area A and Area B is the Grade Ⅰ network node of CL in this building; the BHS machine room is the Grade Ⅱ network node of CL in this building; the Eastern Traffic Hub MDF, the outfield managing center (OMC)MDF, the aviation business administration building MDF is the Grade Ⅱ network node of CL outside this building; while the correlative IDF is the Access Layer. All the core layer, the Grade Ⅰ network node and part of the Grade Ⅱ network node need bi-core allocation(multilink-bind among exchangers). Among core network node exchangers and from network node of CL exchangers to core network node exchangers, bi-link design is used.

The Main-net links to Hongqiao integrated transport public information platform externally, also links to Pudong Airport and Eastern Terminal internally.

Four security-outer-connection is built among four areas: the Western Terminal’s AOC/TOC joint machine room, the Main Distribution Frame of gallery Area B MDF-1, the Main Distribution Frame of gallery Area C MDF-2 and the Main Distribution Frame of Eastern Traffic Hub MDF-TIC, to safeguard a reliable out connection locally.

2.2 Planning and design other sub-network

Commercial POS system can run on the platform. The public commercial areas of west terminal can be covered with network. Inside, it connects with wireless LAN interfaces; outside, it connects with bank, customs and Internet interface.

2.2.1 The security network of the west terminal

It mainly includes hand-baggage and checked -baggage screening systems. The security network of west terminal is designed with two-tier architecture. The core layer is located in security room and the access layer is scattered in the office of votes and the IDF which near the security zone.

2.2.2 The Commercial POS system of the west terminal

It is designed with three-tier architecture, the core layer of the network is located in AOC/TOC joint equipment room, the aggregation layer of the network is located in MDF-1, MDF-2 and MDF-TIC and the access layer of the network dispersed between the relevant IDF.

2.2.3 The wireless LAN of the west terminal

In view of the needs of a variety of wireless applications, the wireless LAN is designed in the corresponding floor of the West Terminal, and in according with the needs of BRS and under the permission of air traffic control nearly 45 seats are covered directional. The visitors in Terminal area and VIP lounge can enjoy wireless Internet and information Inquiry Service by using wireless terminal.

Computer Room A: the computer room of CAAC and China Civil Aviation Information Network Co., Ltd

Computer Room B: the computer room for security inspection information system

Computer Room C: the computer room for baggage management information system

3. Analysis of network security and risks prevention

3.1 Analysis the causes of airport network system security risks

First of all, standing the point of the Hongqiao Airport network infrastructure, we have found that many core components of network infrastructure (such as the main network and server subsystems, etc) ,related technology and application software (for example, large-scale database applications)depend on foreign manufacturers to provide; at same time, some of the airport network security engineers and managers can hardly understand the potential risks, lack necessary technical facilities and related processing experience, so facing increasingly serious network security, they often don’t know how to do and what to do. It is just because of technical limitations, many people only know how to guard against viruses but lack overall awareness of network security,.

Secondly, when the airport is under constructed, its network hardware facilities and application software in a certain period of time is a relatively safe. However, a variety of hardware and application software when they have been made out can’t be tested out all the flaws or loopholes. With the rapidly development of network technology and application software, some drawbacks and vulnerabilities of hardware and software will be exposed gradually. Because hardware and software lag behind when technology is making progress, the network security risks are inevitable.

Thirdly, some man-made factors also threaten with the airport. Man-made network intrusion makes the maintenance of the airport network security to be very difficult, How to deal with all kinds of cyber crime is a good example. Some hackers are taking network system to paralyze as their goal; some lawless are developing those malicious program (such as deleting or changing, even theft the information which is related to airport), these forces can not be disdained.

Finally, there are unconventional threats with network security, such as natural disasters or terrorist attacks, these are unexpected threatens.

Therefore, we need a comprehensive understanding of the airport network threats, taking effective measures to prevent and combat these threats in time. The rapid development of aviation industry asks for more stringent, conscientious and careful airport network security than before.

3.2 Different perspectives of the network safety precautions

3.2.1 Based on TCP / IP protocol security

TCP / IP protocols are a four-tier architecture, which includes the application layer, transport layer, Internet layer and network interface layer. But essentially, TCP / IP has only three layers, namely, application layer, transport layer, Internet layer, because the bottom layer of the network interface has no specific content (Xie Xiren, 2003). However, in according with the specific network layout of the airport, according to the characteristics of the construction of the airport network and TCP / IP architecture, airport network can be divided into the corresponding network application layer, system layer, network layer.

(1). Application layer security. As directly providing service to Application process, application-layer has many protocols in the Internet, such as the World Wide Web's HTTP protocol , supporting for SMTP e-mail protocol, the FTP file transfer to support the agreement, ect (Xie Xiren, 2003). In accordance with these agreements’ function, we can prevent the possible loopholes by use of software methods (see **3.2.3**) to prevent the virus from the erosion and illegal users' visiting; In addition, establishing data backup systems, which make the network can rapidly recover when network has failed to work, and minimize data loss.

(2). System Layer security. Frequent exchange of visits exists in Airport network (including the exchange of visits emerges between Hongqiao Airport and Pudong Airport), a wide range of Resource sharing make the virus more easily transmitted. To protect security of Layer system, first of all , the security of servers need to be protected. Each server has its dedicated software and a dedicated service, in order to prevent the server from attacking, the best way is to close unnecessary services and ports which leave no opportunity to hackers (Qin Ying, 2007). Secondly, checking the backup server's system log regularly, recording the users' operation, analysing log files, reforming the hidden danger of system in time and nipping in the bud. In addition, study show that 80% of network attacks and worm attacks come from internal LAN, the viruses and Trojans have the characteristics of self-replication, so those infected computers will often affect other LAN users. Also now there are a lot of rebound Trojans, which can take the initiative to connect the client and publish harmful information. So in the implementation of security software, firewall software and precaution Trojan horse software should use coordinately. The practice shows that this method will protect your computer from viruses effectively, Trojan horses and other malicious code threats, as well as the invasion of illegal users.

(3). Network layer security. The main function of Network layer is to provide communications for different hosts, and its detailed functions will not be repeated here. During sending data packet, segment network layer composition is packaged into groups or packages by network layer, so is user data. In general, the network layer security can be considered from the following aspects: One approach is to use IP packaging technology, the nature of the package is that plain text is encrypted (a kind of security in 3.2.3 Software-Based Security), encapsulated in the outer layer of the IP report, when it used to encrypt the packets routing on the Internet to reach the other side, the outer IP header has been opened, that is to say, the messages be decrypted (William Stallings, 2002); Another method is to make reasonable use of VLAN division, the VLAN is unrelated to position, making the airport network divide into virtual VLAN network segments, which can suppress broadcast storm on the network effectively; The third way is IP address binding, IP address management is an important part of the network construct in LAN network of the airport. The final paragraph into the address corresponds to the VLAN, at the same time , the IP address of network nodes, and MAC address of equipment are bound. The IP address management methods have greatly improved the safety rules and the availability of traffic control rules, reducing the LAN IP attacks possibility, and improving network security and reliability.

IPSec security measures is also very important to protect the network security, who offers a Clear structure, considering its security, identity validated, integrality, secure secret keys changing, and protection measures (So-Hee Park, Jae-Hoon Nah, and Kyo-Il Chung, 2005). IPSec is widely used in organizations or enterprises to build VPN(Virtual Private Network). IPSec in the IP layer achieves its security services and protects directly all data packets in order to achieve security purposes (Deng Lei, Ai Jisong, 2009).

3.2.2 hardware-Based Security

From the aspect of hardware to address the airport network security, in the design of the airport network system we conduct from the following aspects.

(1). The location selection of the AOC/TOC core computer room need to be relative covert and secure (Of course, geographical location should also be reasonable, in order to network calling), which is basic preconditions of the airport network system's safety. This requires the location selection of the AOC/TOC core computer room to have a certain security and construction safety. On the one hand, it can prevent the interference or destruction of the lawless elements. On the other hand, it can withstand some natural disasters. In addition, we should choose stable capability and reliable quality brands in purchasing the AOC/TOC core network to promote the safety factor of the airport network system.

(2). In order to ensure all the main airport networks and subnets to run 24 hours all day, the airport network servers (especially the AOT / TOC core network server) implement a Hot-Standby hot backup mode (Wu Nian zu, 1999) that is, in the normal situation of the server, a backup server is in a waiting state that once the server on work breaks down, the backup server wakes up immediately, automatically replaces broken-down server to work, and recovers the normal operation of the whole network system, in order to achieve continuous communications of the whole network, then it can meet the airport's requirement of 24-hour continuous work..

(3). Taking hardware firewall to protect the airport network system effectively. It can provide a physical and logical isolation for the external and internal network; what's more, it can be multi-layered defense. In addition, a hardware firewall (especially high-end firewall) can also provide better remote management capabilities except the defense of the internal network security threats. Hongqiao Airport and Pudong Airport will eventually implement the sharing of the information and the unified configuration, which requires interconnection in the network system. Constructing in this remote LAN structure, hardware firewall is essential.

(4). For the high level data security, physical isolation is a good choice (all types of hardware firewall is not absolutely safe. For example, a firewall can not detect encrypted, and the capability of prevention Web applications is insufficient).That is to say, the relative and connected LAN with high security level should not be connected to the Internet, in order to prevent lawless from using the loopholes to access to these data.

3.2.3 Software-Based Security

Carrying out hardware security precautions, software security should be done as well. Combining current technology, the solution is as follows:

(1). Installing anti-virus software. Anti-virus software is an essential part of network security procedures. Before Hongqiao Airport AOC and Pudong Airport AOC connect with each other, it's inevitable that there are software vulnerabilities that haven't been checked out during software testing(Because many systems that are used don't came from the same software company, when information is delivered between different systems , "seamless" is emerged, what's worse, it is a step in the virus), so a safety hazard have broke out. Correct configuration and enforcement anti-virus software can reduce the harmful of networks malicious programs. The administrator should examine virus alarm log regularly, and learn the whole situation of network virus timely, accurately, and remote scanning the threat of computer. In this way, we can prevent the spread of the virus in the local area network effectively.

(2). Network information encryption. Taking into account the safety of network information, encryption has been implemented for data transmission and information storage. The purpose of encryption is to protect network data, documents, passwords and control information, and online transmission of data. After the encryption of systems information, it will protect the information that can not be malicious acquisition and be made use of during transmission and storage.Information encryption coordinate with firewall technology which is used to enhance information systems and information security and confidentiality is one of the key technologies. When the Hongqiao Airport project have been complete, the data of Hongqiao Airport AOC and Pudong Airport AOC will have backed up each other. Switches is the core of two LAN, VTP protocol attack is a threat to the security of switch. VTP domain has been encrypted, so someone haven't know the password or password is incorrect, switch will not be able to learn the news of VLAN. This can effectively prevent VTP protocol attacker entering each of the other users, who are in the same VLAN.

(3). Access Control. Access control is to identify legitimate users own the authority of the system resources, in order to prevent the illegal invasion and legitimate users using non-permission resources, which is the core of application-layer security architecture (Zhang Yun, Kong Fang, 2005). At present, there are many solutions of access control, such as MAC address filtering, VLAN isolation, access control list which bases on the IP address, etc. Each computer system which is belong to the airport network has user access control, as soon as file access permission rights are set. File access control restrictions will effectively carry out legitimate user access to acts within its competence, which maximize the sharing of resources. Implementation of access control information can safeguard the integrity of the information; reduce the HIV infection the opportunity; slow down the speed of the spread of infection; protect the confidentiality of important information and so on.

(4). Intrusion detection. Check whether there is breached strategy behavior or attacked signs by collecting and analyzing computer network or some important information of computer system. The combination of detection software and hardware of intrusion is called Intrusion Detection System(IDS).IDS plays a warning role in network security. Hongqiao Airport West Terminal will provid wireless Internet area, which makes passengers surf the Internet conveniently. However, such opened network also make network security system be in risk, At this moment, it's time for IDS show its function. Whether visitors have illegal intention can be analyzed, thus the corresponding information are feed backed to system control center which judge the visitors are legitimate users or not, ultimate, determine to give access rights if the visitors are legitimate, otherwise refuse being visited.

In a word, to ensure network system security no matter from the TCP/IP protocol architecture perspective or from analysis of hardware and software perspective, they are carried out interlaced when they defense network security. Therefore, all aspects of technical factors are the inevitable choice of implementation countermeasure (as illustrated in Figure 3).

Some special attention should be paid that man factor is the premise of all factors. We have advanced technology and equipment to maintain airport network security hardly enough, reasonable management system, administrator's operation habit, and the safety awareness of network security are the indispensable supplement.

4. Conclusions

Airport network is a quite complex system engineering, with the improvement of technology, ensure airport network security is a dynamic and perfection process. In order to solve this problem, first of all, we must think about from different angles and multiple levels, adopt diverse security measures; secondly, both the openness and security of network should be considered, understanding the potential threats in the network, analyzing network structure deeply in any times, making out suitable and reasonable management programs on the base of actual situations, carrying on protection network from the whole aspect, that's to say, we should defense airport network security with the means which will have coordinated all aspects of the technological superiority, only in this way can make network in the maximum safety and ensure airport network system security, stable and efficient operation.

The construction of Hongqiao Airport West Terminal network system have been first-class in the domestic at present, studying and summing up this experiments have the role of inspiration and setting a model to domestic airport construction in the future.

5. Acknowledgements

This research was supported by the research project of Science and Technology Commission of Shanghai Municipality of China (No. 06211212051). Expresses the thanks.

References

Deng, Lei & Ai, Jisong. (2009). A Study of Automatic Generation of IPSec Security Policies. *Computer Security*, 2009(1): 4-8.

Qin, Ying. (2007). Airport Research on Design and Application Technology of Airport Network Security. *Jiangsu Aviation*, 3(2): 32-33.

So-Hee Park, Jae-Hoon Nah, and Kyo-Il Chung. (2005). The Implementation of IPsec-Based Internet Security System in IPv4/IPv6 Network. LNAI 3397: 109-116.

William Stallings. (2002). Foundation Course of Network security. Beijing: Tsinghua Press.

Wu, Nian zu. (1999). The Construction of Pudong International Airport—Information System. Shanghai: Publishing House of Shanghai Science and Technology.

Xie, Xiren. (2003). Computer Network(The Furth Edition). Beijing: Publish House Of Electronics Industry.

Zhang, Yun, Kong, Fang. (2005). Design and Research of Application Layer Security Architecture. *Microcomputer Development*, 15(3): 16-17.

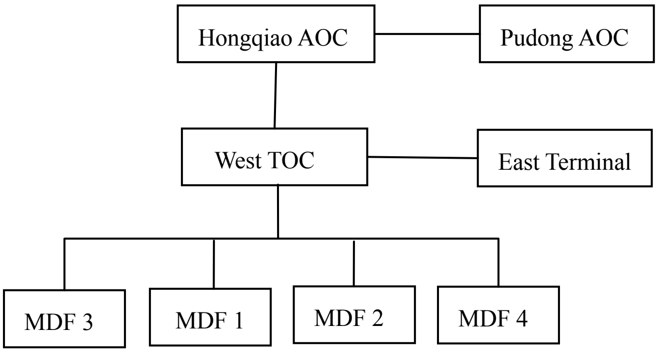

Figure 1. main network plans

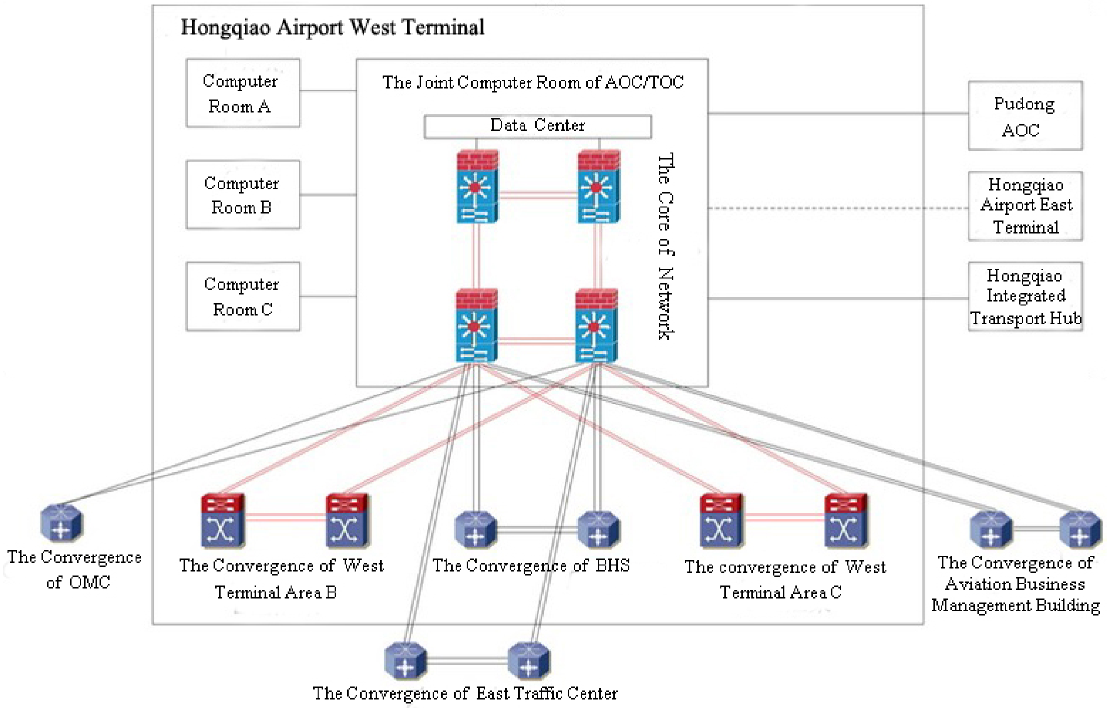
Hongqiao Airport West Terminal
Computer Room A
Computer Room B
Computer Room C
The Joint Computer Room of AOC/TOC
Data Center
The Core of Network
Pudong AOC
Hongqiao Airport East Terminal
Hongqiao Integrated Transport Hub
The Convergence of OMC
The Convergence of West Terminal Area B
The Convergence of BHS
The convergence of West Terminal Area C
The Convergence of Aviation Business Management Building
The Convergence of East Traffic Center

Figure 2. Hongqiao west terminal core network of main network

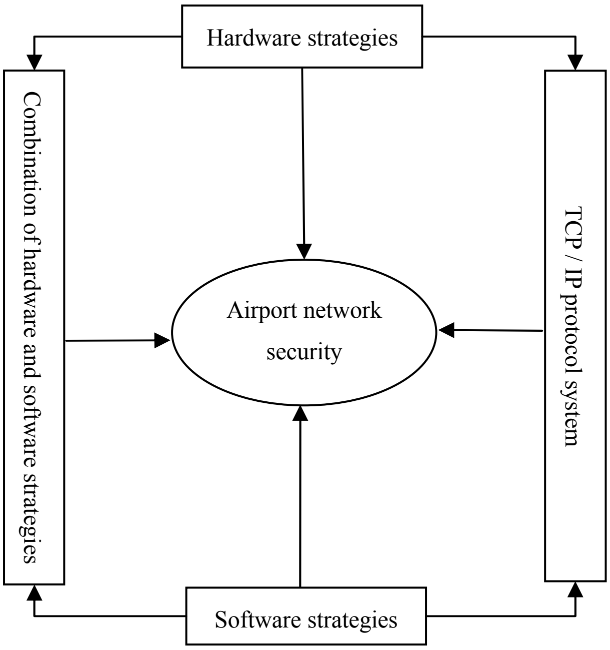

Figure 3. Coordination of the strategy to maintain the airport network security