Security Policy on Logistics Management Information System Based on Web

Linna Huang, Fenghua Liu
Department of Computer Engineering
Cangzhou Normal University
Cangzhou, China
Hln0322@163.com

***Abstract*—With the internet development and further development of information technique applications, information management system is used more and more widely in logistics enterprises, but consequent security issues of network information have become increasingly prominent. The paper was set in information system of logistics management of some company; security problem of application system in logistics enterprise under network environment was studied, and security architecture of logistics management information system and specific design program were introduced.**

Keywords- logistics; management information system; security; policy

I. IMPORTANCE OF INFORMATION SYSTEM SECURITY ON LOGISTICS

Logistics management information system is a man-machine interactive system which is composed of staff, hardware and software of computer, network communication equipment and other office equipment, and its main function is to make collection, storage, transmission, processing and sorting, maintenance and output of logistics information to provide supports of strategic, tactical and operational decision-making for logistics managers and other organizations managers. Currently, more and more logistics companies have established logistics information system of their own, and used Internet to develop business management and information services, so that operational efficiency of inner enterprises and customer service quality are not only improved, and reaction speed of market, decision-making efficiency and comprehensive competitiveness of enterprises are also improved. To logistics enterprises, security of networks and information systems data is premise and foundation for normal sustainable development of operating activities, therefore, various security technologies are fully used to establish a multi-channel strict safe defense-line, and it is very necessary to maximize security protection of management information system and all data of logistics.

II. SECURITY SYSTEM HIERARCHY OF INFORMATION SYSTEM ON LOGISTICS MANAGEMENT

A complete system of network security is divided into different levels and different levels reflect different security issues; according to system structure, security system of information system of logistics management can be divided into five levels, namely: security of physical layer, network layer security, security of system layer, application layer security, and manage security [1] and Figure 1 shows relationships among various levels.

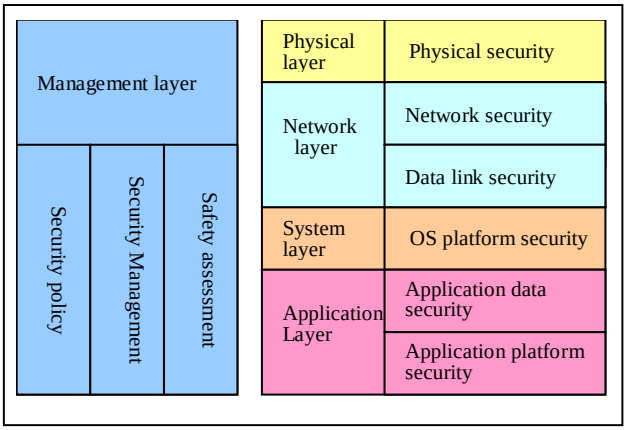

Figure 1. Security levels relationship of logistics management information system

A. *Physical layer security*

Physical layer security includes computer room safety, safety of a variety of physical devices, communication line security, etc. The physical layer is the basis for building information network and network transmission, and thus the security of physical layer is starting point of all security. But physical layer is the most overlooked of all constituent elements of network facilities; people tend to focus more on management and service of higher-level network structure, but ignore foundation-physical layer of network transmission. Physical layer security is mainly in the security of software and hardware equipment, reliability of communication line, anti-disaster and anti-jamming capabilities of equipment, device backup, operating environment, guarantee of uninterruptible power supply and other aspects.

B. *Network layer security*

The network layer is pathways and channels for information systems offensive by network intruders, so many security problems are reflected in the security aspect of network layer. Network layer security includes: security of network topology structure, ID authentication of network layer, network scanning technology, firewall technology,

confidentiality and integrity of data transmission, remote access security, routing system security, security of domain name system, real-time intrusion detection means of network, etc.

C. System layer security

The security of operating system is also known as host security, and main show is in the following three aspects: ① computer virus has a threat to operating system. ② operating system has its own shortcomings and vulnerability, resulting in security risks, such as system vulnerabilities, ID authentication, access control, and so on. Code of modern operating system is large, and all OS have security holes in varying degrees, and security vulnerabilities of some operating systems are better known, such as Unix, Windows NT, etc. which are widely used. ③ security configuration issues of operating system are as followings: system administrators or users do not know enough about complex security mechanisms of operating system and incorrect security configuration settings related to system can also cause a security risks.

D. Application layer security

This level security is built on the basis of security of network, operating system and database. Network application system is complex and diverse, although security issues of some special application systems can be solved using a specific security technology, such as Web applications, database applications, e-mail applications, etc., but due to critical business (such as transaction management control, decision analysis, etc.) system and important data of many enterprises all run on database platform, and then, if database security can not be guaranteed, the application systems that run on it will be destroyed or unauthorized access.

E. Management layer security

Institutionalization of management is an important guarantee for information systems security of entire network management. Strict safety management institution, reasonable staffing and clear partition of security duties can largely reduce other layers security risk. Management layer security includes security management of device, decision and implementation of security management institution, organization regulation of departments and staff, risk assessment, security evaluation, etc.

III. THREATS TO SYSTEM SECURITY OF LOGISTICS INFORMATION MANAGEMENT

A. New features of attacks upon application layer

1) Strong concealment: attacks on Web applications are complexities which are started using Web vulnerabilities, including SQL injection, cross-site scripting attacks, etc., and a common feature is strong concealment and not easily found.

2) Attack for a short time: a data theft, a Trojan planted or control on entire database or Web servers is completed in just a few seconds to a few minutes.

3) Big perniciousness: Almost all banks, securities, telecom, mobile, government and e-commerce companies provide online transactions, queries and interaction services now. User's confidential information includes account, personal private information (such as identity information), transaction information, etc. which are all stored in back station database via web, in this way, once online server is paralyzed, or although it is in normal operation, background data have been tampered with or stolen, the two conditions will cause huge losses of enterprises or individuals.

B. Shortcomings owned by traditional firewall or IDS products

1) Firewall: access control is realized through port restrictions, but to web applications, its HTTP/HTTPS port is open. Therefore, firewall is unable to detect occurrence of attacks on Web application, let alone prevents attacks.

2) Intrusion Detection Systems (IDS): known attacks are detected which relies on signature database, but for attacks on Web application, there are a great many deformations (for example: SQL injection, cross-site scripting, malicious file inclusion, etc.), so IDS can not limit all features, of course, it is also impossible to predict future deformation.

C. Problems in system management, technology and audit levels

1) At management level: Problems represent that staffs have duties; process needs to be improved; day-to-day operation of internal staff needs to be standardized; operation and monitoring of third-party maintenance people is failure, etc. so when security incidents happen, it is unable to trace and locate real operator.

2) At technical level: On the one hand, to protect security of database information, the corresponding management institution is worked out, but there is no corresponding technical means to control it; on the other hand, when database is installed, phenomena are widespread, including the use of default configuration, default passwords, default permissions, etc. from database vendor. Operations inside existing database are unknown, so malicious actions, resources misuse and disclosure of enterprise confidential information of internal users can not be prevented by any external security tools (for example: firewalls, IDS, IPS, etc.).

3) At audit level: Audit function [2] is that all operations of all users on database are recorded in audit log. If malicious modification, destruction or deletion, etc. illegal operations appear in database, and the operating event is analyzed and the staff is traced through information recorded in audit log. However, there exist many drawbacks in existing audit method which is dependent on log files in database, such as that: open of database audit function will affect performance of database itself, and the being tampered risk with exists in database log file itself; it is difficult to reflect authenticity of audit information.

Published by Atlantis Press, Paris, France.

With exaltation of data value as well as enhancement of database accessibility, internal and external security risks are greatly increased which database faces, for example, illegal unauthorized operation and malicious intrusion lead to leak of confidential information, etc. which can not be effectively traced and audited after the event.

IV. SECURITY PREVENTION STRATEGY OF LOGISTICS MANAGEMENT INFORMATION SYSTEM

A. *ID authentication*

ID authentication, also known as "validation", "authentication", means identity confirmation of user [3] is completed by certain technical means, and user name and password identification is the most common way in ID authentication. User name and password is a security measure for permissions management and access control in database management system. Windows authentication and mixed authentication mode of information system authentication of logistics management combined with SQL Server authentication are adopted in system design.

B. *Installation of anti-virus software*

A most important step of network security construction of logistics enterprise is prevention of computer viruses. Using a variety of anti-virus softwares prevent virus from invading system, which is safety precautions that is most familiar to people. In addition, virus prevention also needs perfect management practices, such as that: pirated software is not used; email from unknown sources is not opened, and unreliable websites are not visited; access permissions or encryption is set for important documents; for particularly important data, backup protection is made at any time; anti-virus software is upgraded in a timely manner and virus is regularly killed; etc. In specific design of logistics information system, we selected Norton Enterprise Edition antivirus software and combined it and related anti-virus system to effectively guarantee system security.

C. *Allocation of firewall*

Firewall is a preventive technology which is most widely used [4], the combination of a series of components which are set between internal network of trusted enterprise and untrusted public network, protective barrier of network security, and also effective means against hacker attack, so that risk can be reduced by filtering unsafe services and the security of internal network is enormously improved. Firewall is a limiter, separator, or a parser logically, can effectively monitor activities between Internet and internal network, and provide security guarantees for internal network. We chose Rising Firewall and combined it with other technologies to build a network protection system in information system of logistics management design.

D. *Security mechanisms of database*

Database is the foundation of information management system, to logistics companies, all contracts, orders, and transaction information are stored in database, and thus database security should be paid more attention. Database security means that database is protected to avoid illegal use, and leakage, destruction or alteration of data is prevented, which are mainly reflected in following aspects: ① existence security of database; ② database availability; ③ databases confidentiality; ④ database integrity.

Database security mechanisms can be divided into four levels, namely: user layer, database management system (DBMS) layer, operating system layer, database layer, where: ① security mechanism of DBMS layer is achieved through access control, that is, access permission of different users to a variety of objects is set in database, which is the most effective security means of database management system and also core technology in database security system. Access control can be achieved through user classification and data classification. ② Most security mechanisms [5] of database layer are guaranteed by encryption technology [6-9]. Database encryption is the most basic prevention technology to prevent information distortion in the network system, and also the last defense line of data security. In actual system design, we selected Microsoft SQL Server 2000 as database management system, adopted encryption granularity as data storage encryption way of field, achieved user access based on roles and passwords and ciphertext transmission of information in network, so security of database system is greatly improved.

E. *Data backup*

Data security is a core part of information system security of logistics management, which has two meanings: the first is logical security, and the other is physical security. The former requires security protection of system, and the latter needs protection of data storage backup. Data backup[10,11] is the last line of data availability to guarantee data recovery after failure (mainly system failure) occurs. If there is no data backup, it is impossible to recover lost data, resulting in an immeasurable loss. Regular backup of database is most reliable and cheaper way to prevent system failure and can effectively recover data. Database backup methods that are often used include hot standby, hard disk mirror backup, etc. For a complete strategy of database backup, it is necessary to take into account a number of factors, including: backup cycle; use of static backup or dynamic backup (dynamic backup that also allows to make database backup in runtime); use of full backup or combination of incremental backup; backup media; manual backup or system automatic backup; etc. For cost reasons, we have adopted a more economical form of restore anywhere, and used automatic backup function of Ms SQL Server 2000 and transfer tool of restore anywhere to achieve data storage backup, selected suitable backup plan based on the business volume of logistics enterprises or important degree of data, and set timer (weekly, monthly, daily or hourly) that database data in server are automatically sent to database of another workstation machine by a computer. Moreover, it is also necessary that some tables or all data are regularly backed up to an optical disk or U disk for safekeeping.

F. Management-level security

Security guarantee of logistics management information system is decided by technology, management and human role jointly. Security is limited obtained using technical means after all, and all strategies, technologies, tools use and management have to rely on people, therefore information system security of logistics management is essential from prevention of management level. It is necessary to make an institution of systematism security management, such as: security backup of information systems and correlative operating procedures; security management institution of systems and databases; use authorization of networks, network detection, network facility control and related operating procedures; etc.

V. CONCLUSIONS

With rapid development of economy, information technology and Internet as well as informatization processes being constant to deepen, networking has become the inevitable choice of informatization development of logistics enterprises, and logistics management information system has been widely used; informatization throughout logistics decision-making, business processes and customer service has brought a great promotion to development of logistics enterprises. However, the security problem of network information system emerges, then how to guarantee safe operation of logistics management information systems is a challenge logistics enterprise faces in development process of informatization.

Advantages and disadvantages, and emphases vary in above various security safeguards; one technology can only solve some facet of problem, but mutual integration of a variety of technologies and effective implementation of related management measures is fundamental way to build a security and strong logistics information system. Security protection of logistics management information system is multi-layered system engineering, and only a comprehensive application of a variety of techniques, strategies and management measures can achieve effective protection purposes.

REFERENCES

[1] Gu Yongtao, Ge Lihong, and Ju Shuchun, “Analysis to Safety of Electric Power System Information Network,” Inner Mongolia Electric Power, vol. 28 (S2), pp.18, 2010.

[2] Wu Huili, and Fang Jiajuan, “The Research of Datebase Security Technology Based on Web,” Information security and technology, pp.8–10, August 2011.

[3] Han Jingfeng, “Study on Security Policy of Computer Network Database,” Information security and technology, pp.3–4, August 2011.

[4] Zhi Hecai, Yu Yanming, “Study of Web-based Database System to Prevent Intrusion of Technology and Countermeasures,” Coal Technology, pp.239–240, September 2011.

[5] Lin Ming, Ye Qing, and Qin Wei, “Analysis of Datebase Security Technology Based on Web,” Information & Communications, pp. 90–91, April 2011.

[6] Hou Youli, “Three-tier Structure Design of Database Security,” Communications Technology, vol 44, pp. 118–120, April 2011.

[7] Luo Changzhuang, “New Thinking on Data Encryption Methods,” Computer Era, pp.17–18, September 2010.

[8] Ma Hao, Wang Xiaoming, “Security Access Control Mechanism of Outsourced Database,” Computer Engineering, vol.37, pp.173–175, May 2011.

[9] Chen Guang, and Zhang Xikun, “Research and design of algorithm based on data encryption,” Information Technology, pp.148–152, May 2010.

[10] Lin Rudan, and Chen Lanzhen, “Brief talk on construction of data security guarantee system of hospital information system in network environment,” Science and Technology Innovation Herald, vol 20, pp.237, 2010.

[11] Liu Chunli, Huang Linna, and Tang Lifang, “Computer Network Security and Countermeasures,” Coal Technology, vol 31, pp.170–171, July 2012.

Published by Atlantis Press, Paris, France.