Discussion on Security Policy of Dam Safe Monitoring System based Network Environment

Xiaohua Zhang[1], Zhaohui Zhu[2]

[1]Yellow River Institute of Hydraulic Research, Research Center on Levee Safety Disaster Prevention Zhengzhou, china

[2]Engineering Safety Monitoring Center, China institute of water resources and hydropower research Beijing, china

Keywords: Dam, Safety Monitoring, Information Management System, network, security policy.

Abstract. Nowadays, functions of Dam Safe Monitoring Information Management System are unceasingly strengthening and computer network is rapidly developing, while the problem of system and data security is day by day prominent. This article summarized current development situation of Dam Safe Monitoring Information Management System, analyzed a series of security problem which the system faced under network environment, and proposed a set of more perfect security policies with characteristics of the system.

1. Introduction

The safe operation of dam is very important to social stability, security of lives and properties, so most medium-sized hydraulic projects have installed the software of safe monitoring system. With the development of safe monitoring system that software and monitor database, the government management department and society start to pay more and more attention to the monitoring system and the safety of information database. Although the network is very convenient to people, it makes malicious attack and threat to system and database. If the treatment is not very efficient, the consequence maybe is very serious.

Although system safety has primarily been considered by many LAN and enterprises, the planning and designing of dam safe monitoring system are just focused on the system's functionality and reliability, not enough attention was paid to the safety problems. The main contents of this article are security needs, security threats and corresponding countermeasures of dam safe monitoring system which is under the network environment.

2. The system architecture of dam safe monitoring in information management

Figure 1 shows the information management structure of dam safe monitoring, in the center is the switch which is the bridge of the various' components and transmission. On the left and top of the switch is the data acquisition system which is consisted of various monitoring sensors, control unit and data acquisition machine. Collected data eventually is stored in the database server for information management, analysis and decision support. On the right of the part is WAN users, mainly referring to living off-site experts and engineers who can complete the remote analysis, diagnosis and decision supported by internet. The Lower left is the management department of the other internal LAN dam and hydropower station, who can share the data from the server. The below is the system terminal, which provides a platform for the system users. The one on the right is the server farm of the system, including Web server, database server and application server. Among them, the web server provides query function access for the Internet/Intranet users, the application server provides information management systems, analysis, evaluation and decision support for the system customers, the database server provides underlying data support for Web and application servers.

Modern computer network makes security dam safe monitoring system advanced, which mainly reflects in the following aspects: it can search all the online resources rapidly, realize abnormal and decision support, improve the reliability and accuracy of diagnosis by cooperative consultation of

many experts, through shorting the space distance and the realization of remote data transmission, can not only save time, but also reduce the cost; all these achievements enable the sharing of knowledge, information and data.

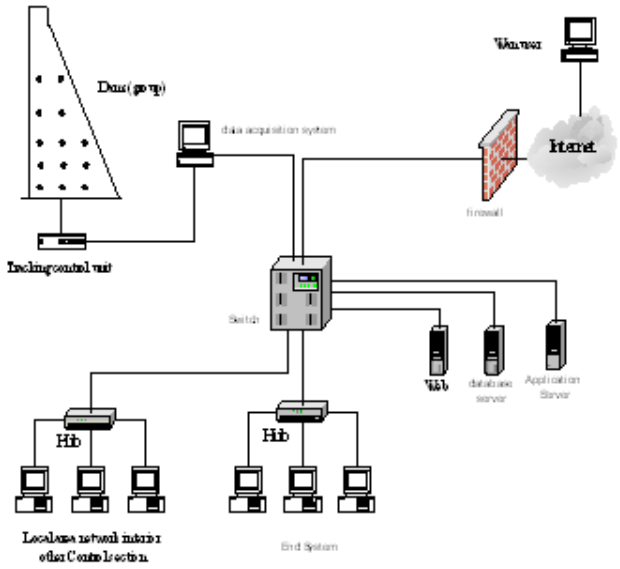

Figure 1.The physical structure of dam safe monitoring in information management system

3. The threat of dam safe monitoring in information management

3.1 The security summary of computer and network

International Organization for Standardization (ISO) gives the definition of computer security: it is the safety measures of technology and management for data processing system, protecting computer hardware, software and data from damaging changing and revealing due to the accidental and deliberately causes. The system of dam safe monitoring is consisted of system hardware and system software, computer hardware is the carrier of system; system software manage and control the computer inside data, which provide necessary methods and ways for computer data transmission and exchange.

Resources sharing and service to users are the most important resource of computer network, so the definition of security is: by taking a variety of technical and managerial security measures to ensure the availability of network services and integrity of network information. The former requires the network to provide network service selectively for all users at any time, the latter requires the network to ensure the information resources' integrity, availability, accuracy and limited dissemination.

3.2 The threat of dam safe monitoring in information management

Management system is imperfect. The imperfect of management system is one of the important sources of network security. For example, the network administrators' arrangement is not very suitable, employees' safety consciousness is weak, the user password setting is unreasonable, the management system is not perfect, etc, which will pose a serious threat to information security. The safety awareness of hydropower station information managers is relatively weak, which is mainly reflected in: the trust to anti-virus software and firewall are so much that the prevention measures to security threats from internal are not enough, over-reliance on technology, such as physical isolation, the knowledge of new information security problems is not enough, etc.

Physical security risk. The unexpected incidents caused byflood, fire, lightning, etc; the instruments are damaged, stolen and destroyed for human-inducing.

The security risks of operating system and application software. For operating system and application software, there are some security vulnerabilities, which be utilized to attack network. The security vulnerabilities include security management vulnerabilities, operating system (Windows,

UNIX, Linux) vulnerabilities, database system vulnerabilities, application system vulnerabilities, network management vulnerabilities, etc.

The risks from internet. One of them is malicious attack, for some motivations, on the Internet some users invade and attack systems and equipments of the station's computer, which result huge losses by affecting the information transmission between hydropower station's local area network, destroying software systems and data, stealing hydropower station's confidential information. The others attacks have no general purpose, such as viruses, worms, Trojans and spy ware, etc, which are the most vulnerable to the current network security issues. These threats include interception, interruption, tampering, counterfeiting, and malicious programs, etc.

The risks from dam and hydropower station internal management department. With similar risks from the internet, one is attacking the system by internal staff or collusion which is the most deadly threat, the other is the misuse or abuse caused by negligence, which requires strict management system and improve staff training system, also needs the system itself has some abilities for error correction and fault tolerance.

4. System security policy

System security strategies include all activities and measures for ensuring the security and information network. Security strategy is a systematic and global problem. Hydropower and dam structure is so large and the relationship between managements is so complex that it is very difficult to consider security strategy. The following article will explore security strategy of dam safe monitoring in information management system from several perspectives.

4.1 The overall planning of network security system

security protection strategy: the relationship between internal LAN and the Internet is external physical isolation or Logic isolation, if it is logical isolation, operators must pay attention to firewall which is not panacea, in addition, the firewall should be noted here and need to be updated periodically, which can greatly prevent viruses and malicious attacks, select appropriate operating system and application software to minimize security vulnerabilities, dense security classification of the data, what data can be changed by the user, what data is allowed to publish to the Web, need to be clearly defined. The system settings and place of application server and database must be reasonable and safe, designed to protect computer systems, network servers, printers and other hardware entities and communication links from natural disasters,vandalism and online attacks.

security recovery strategy: Although the original system architecture models could meet the need of monitoring information, processing data calculation and prediction, monitoring alarm processing and knowledge representation, interpretation and output, etc, the system architecture need to be improved and perfected due to the development of network functions. For the security reasons, the database's backup is increased, which is isolated form system database. The system database is copied by security strategy mechanism.

4.2 Personnel safety awareness and rules' complete

Attention to the improvement and development of management system, strict enforcement, safety training for operating personnel. To ensure system security, the necessary technical means are important, however, the technology is not a panacea, the strict management system is essential. Therefore, the enterprise network security, security management and system construction is very important (especially for internal network). Strengthen the education of operations and network management's safety consciousness instruct, all staff to consciously observe and implement all national policies, regulations about security, compliance the security system of network operation and using, form good operating code.

4.3 Technical means of security policy (including access control, encryption, authentication, attack detection, fault-tolerant error correction system, database backup, honeypot technology, etc.)

Remote data transmission uses data encryption and authentication technology. Encryption refers a message (or plaintext) to be converted into a meaningless ciphertext, which is encrypted by the

encryption key or function. The receiver will decrypt this ciphertext by encryption function or decryption key. The process shown in Figure 2. The encryption Key is selected from a large random numbers, which is divided into two kinds by the encryption algorithm, private key and public key. Private Key is also as known as symmetrical key or single key, which encryption and decryption use the same key (algorithm), such as the DES algorithm and MIT Kerberos. Communicated with the multi-use, single key will produce so many keys that it is difficult to manage. Public key, also known as asymmetric key, uses the different key (algorithm). Data encryption and authentication technology has been used more and more in remote transmission of dam safety monitoring. Data is encrypted at the sender, decrypted at the receiving end, which can prevent the data from being stolen by the third party.

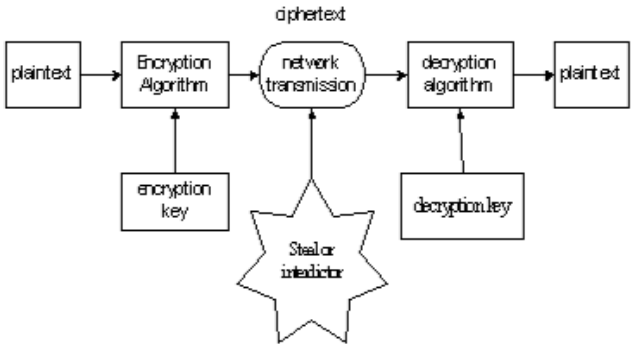

Figure 2.the process of Information encryption transmission

Intrusion detection and active defense technology. Intrusion detection is that finding the intrusion behavior, through collecting and analyzing information with the computer network or computer system, found whether has the behavior of violating the security strategy or signs of being attacked for intrusion detection software and hardware, which is the intrusion detection system. IETF(Internet Engineering Group) divide intrusion detection system into four components: EventGenerators, Event Analyzers, ResponseUnits and EventDatabases. Event Generators are set at the entrance of dam structures safety monitoring system, once a user wants to enter, will be recorded. Through analyzing the user's action, he will be tracked and defended once he has dangerous actions, which analyze method is similar to log subsystem method.

Set the trap, lure him deeply, use honeypot technology. Honeypot technology is as one of the methods to stop hackers, which is a new popular technology. Honeypot is defined as: a resource to attract and trap valuable, which seems to be detected, attacked and potentially exploited. In dam safety monitoring system, honeypot system and monitoring system’s subject is in the parallel position, but the honeypot system does not fix any security system vulnerabilities, so the intruder has some confusion, it demonstrate to the intruder that the information is false or wrong. In accordance with the degree of interaction between the intrude and honeypot, honeypot can be divided into low-interaction honeypot and high-interaction honeypot. The low-interaction honeypot can only complete simple interactions, usually by simulating some services or operating system to work, the intruder's behavior is limited to analog level. The high- interaction honeypot provide a real operating system and applications, so the intruder will have more room, also can get more information of the intruder. But the risks are greatly increased, if the honeypot is compromised, intruder may use these systems as a springboard to attack other systems or databases, so it must be controlled by necessary means.

Through timely and immediately copying database, the safety degree of system data. is increased. There are two security threats from the outside, one is to damage the system, which can cause paralysis of the system, the other is to damage the database, which can alter or delete data. The second situation is very dangerous, if the database is not copied, the important historical data will be permanently lost, which will result in incalculable losses. Therefore, it is very important to timely and immediately copy the database.

In the security strategies of dam safe monitoring system, backup strategy is a passive defense system, whose purpose is that enable the destroyed system to return to the state of beginning as far as possible. The author studies two database backup programs: (a) timing backup, the user selects the backup frequency (monthly, weekly, daily ...),backup time and backup way((full backup and incremental backup),the system will immediately set the database backup to a folder, (b) timely backup, with the other operation, the users enable copy databases to any paths at any time. Once the database is damaged maliciously, you can select the appropriate database to restore data.

5. Conclusions

The dam safety relates to the national economy and people's lives. The reliability of dam safe monitoring information management system and dam safe monitoring data will directly affect the dam operational status' judgments of the dam's operation managements, but many dam management departments are not enough attention to the system and data's security, so consciousness should be intensified, which are as fellows, the safety problems of dam safe monitoring information management system and dam safe monitoring data are very complex and dynamic system engineering, the existing security strategy should be constantly updated, in the same time, ought to strengthen the management of related persons, formulate strict rules and use the most cutting-edge safety technology, finally establish a true safety system of dam monitoring information management. Always use the Figure caption style tag (10 points size on 11 points line space). Place the caption underneath the figure (see Section 5). Type as follows: 'Figure 1. Caption.' Leave about two lines of space between the figure caption and the text of the paper.

References

[1] Chang Lin. Safe Services and Security Technologies of Computer network [J]. Chang Chun Engineering College (Natural Science), 2001, 2 (3): 63-64.

[2] E. Becker. Condition-oriented maintenance of vertical roller mills through autonomous telediagnosis systems with e-mail signaling [J], ZGK International, 2000, 53(5):262-268.

[3] Feng Wen, Zheng Binglun, Wu jiang. Based on 802.1x's Design and Implementation of Campus Network Identity Authentication System [J]. Sichuan University Journal (Natural Science) (Natural Science), 2006, 43 (6):1236-1241.

[4] Ju Li. Exploration of network security and protection [J]. Science Information (Academic Edition), 2006 (12):166-167.

[5] Wu Zhongru, Gu Zhongshi. The Expert Systems of Dam Safety Comprehensive Evaluation [M]. Beijing: Science and Technology Press, 1997.

[6] Wang Jian. Research on Key technology of Dam safety monitoring integration intelligent expert system [D]. Nanjing: Hydropower College of Hohai University, 2002.

[7] Wen Hao, Zhou Anmin, Sun Jie. Research and Prevention on Trojan based on Winsock2SPI Technology [J]. Sichuan University (Natural Science), 2007, 44 (1): 81-85.

[8] Wang Lu, Qin Zhiguang. Technology and Application of Business Honeynet [J]. Computer Application, 2004 (3): 43-45.

[9] Xu Lufeng, Zhang Xiaotian, Zhang Min. Research on Information Network Security of Power Enterprise [J]. China Power Education, 2006, Special Issue of Technology BBS Special, 2006: 29-31.

[10] Zhu Zhaohui, Gu Zhongshi,Bao Tengfei,Jing Ji, Research on Dam Safety Monitoring System Software Based on Visual and Component Technology [J]. San Xia University Journal (Natural Science).2007, 29 (6): 486-489.

[11] Zhang Xiaotong, etc. Research on TECO of Remote Diagnosis System [J]. Metallurgical Equipment, 2001, (1): 30-36.

[12] Zhan Chao. Security Technology on Internet [J]. Information Age, 1997, (6): 34-37.