Research on the information security system in electrical gis system in mobile application

Chao Zhou[1], Renjun Feng[2], Haitao Jiang[1], Wei Huang[1], Daohua Zhu[1]

[1]State Grid Jiangsu Electric Power Research Institute, Nanjing, 211100, China
[2]State Grid Suzhou Power Supply Company, Suzhou, 215004, Chian

Abstract. With the rapid development of social informatization process, the demands of government, enterprise, and individuals for spatial information becomes larger. In addition, the combination of wireless network technology and spatial information technology promotes the generation and development of mobile technologies. In today's rapidly developed information technology field, network technology and mobile communication have become the two pillar industries by leaps and bounds. They almost absorbed and adopted all the latest information, communication, computer, electronics and so on new technologies. Concomitantly, the network coverage is more and more big, the transmission rate is faster and faster, the volume of user's terminal is smaller and smaller. What's more, from LAN to WAN, from wired network to wireless network, from wired access to mobile wireless access, people's demand for communication technology is increasingly higher. As a result, mobile communication technology is facing unprecedented challenges as well as unprecedented opportunities. When combined with the existing mobile communication network, it led to the development of leaps and bounds. However, due to the inherent dependence of the system on the existing computer communication network, information security problems cannot be ignored. Today's information security has penetrated into all aspects of life. Information system is a complex computer system, and it's physical, operational and management vulnerabilities constitute the security vulnerability of the system. Firstly, this paper analyzes the composition of mobile enterprise network and information security threat. Secondly, this paper puts forward the security planning and measures, and constructs the information security structure.

1. Introduction

The development of information technology is affecting the development and progress of the whole society, and the communication and network technology are the subjects of information technology. The popularization and application of Internet, rise of mobile communication, and the increasing integration of efforts of satellite communication and various kinds of communication technologies and Internet technologies make the modern communication technology and network technology has made the rapid development. With the development of optical fibre transmission technology and the continuous update of access network technology, the network level of the whole world is increasing day by day [1]. It also promotes the progress and development of various fields of the national economy. At present, the technology development of the world telecommunication industry has

entered a new stage of development, appearing the new trend of integration, adjustment, and reform. In particular, the development and application of broadband technology has become a hot spot for global development in the coming period.

The rise of the information society has further brought opportunities for the rapid development of global information technology. The application of information technology has caused great changes in people's production, life style and concept, which greatly promotes the development of human society and the progress of human civilization, and brings the human into a new era. However, while people are enjoying the enormous benefits brought by information network, they also face the severe test of information security. The existing information security has been a threat to national security, economic security, military security and social security [2]. Because the mobile is the technology dependent on computer network and mobile communication network, the information security has attracted more and more attention. An important geographical location, the leaked military targets and so on are the major threat to national security. From this point of view, this paper discusses the composition of the information network and its application in the process of application, and the relevant security threats and solutions in all links of computer network and communication network.

2. Composition of mobile enterprise network and information security threat

2.1. Importance of information network security

With the continuous development of Internet, it also brings some problems of enterprise network security. With the further development of information technology, both the telecommunications network and other network information infrastructure have become a key technology of information society. They not only service information transmission, but also become the important national infrastructure. Important information systems have been related to the people's livelihood. Information security is not only the thing related to network community and information industry, but has been related to the overall national security. Whether it is economic security, political security, social stability, national security and information security, they are closely related [3]. As a result, to understand the informatization from this global aspect, the guarantee of network and information security work is more important.

The development of information security and information technology is a complementary relationship. The national information security strategy and national information security related deployment clearly pointed out the need for security in the development, to promote the development with security, which is a highly summary for the relationship between the development of information security and information technology. Information security is closely related to the development of information technology, and the development of information security technology is closely related to the overall development of information technology [4]. In addition, information security equipment is also closely related to general information, technology equipment, and information industry equipment. Form network equipment, communication equipment, computing devices to software, many security features and technical equipment itself are closely related, let alone the close relationship between the depth and existence of information security and information technology application. With the deepening of application, it is deeper and extending, so there is close relationship between information guarantee and information security. The relationship suggests that, to do well the management of information security, it is necessary to closely connect the information security with the development stage of information technology. Moreover, it needs certain strategies and practice for information security guarantee at a certain stage of development. Therefore, information security must be understood and practiced from the overall situation of information technology.

Information security technology and concept are continuously developing, and it achieves the security through the network isolation and information encryption in the early stage. After a stage of development, it is found that it needs for coordination for how to balance the application and development by isolation and encryption. In consequence, it entered a new stage. The so called information security stage is to use the security protection detection response, such life cycle, to

achieve the security work. However, with the development of information technology, the popularization of the application is not enough. Because when the network infrastructure and critical information systems need to continue running when they are attacked by human factors or making blockage and obstacles because of natural factors, it converts into the so-called turning survivability stage. Regardless of virus, or attack or natural disaster, the important system needs to continue running, which the process of understanding and development of information security. With the development of information technology and the further development of information security, our theory and technology, concepts and models are deepening and developing.

2.2. Security hidden trouble in Mobile Enterprise Intranet

1) Compared with the external network, the internal network is faster, which can prevent omissions and has simple security measures. Enterprise internal network has the following security risks:
The speed of the internal LAN is fast, the information is easy to be stolen quickly, and the monitoring time is lost quickly;

Internal LAN access is easy. In general, as long as the general information equipment is used, it can be connected to the network;

Internal LAN access authentication measures are simple;

The vast majority of local area network information is not encrypted, making use of plaintext transmission;

Users in the internal network often have the right to operate directly on the database and the server. There is an opportunity to misuse the key data, and to intend to steal or destroy;

Improper use of external devices in computer systems can cause leaks.

Many internal network users do not pay attention to the password, but using a weak password, so the cracking procedure of hackers in the internal network is easier to work;

The internal network is based on the Client / Server way, the client directly operates the server, and the transmission of information in the internal network is very insecure.

2) The internal network data management itself is usually not very strict. Core confidential data generally uses simple protection authority password. In the product research and development process, the various core technology information and job information even have no protective measures. At least for the entire development group, all of the development results and data are transparent and shared. Almost no measures are taken for protection mis-operation, anti-theft and anti-destruction. This makes it very easy to obtain authorization and access to information in the network. The information system with no internal network security management makes anyone may intentionally or unintentionally cause security risks and lead to disasters.

3) Lack of effective management mechanism. Enterprises often lack a more effective management mechanism to effectively manage the internal security [5]:

The internal security management mechanism is imperfect. There are a number of effective management mechanisms within the enterprise, but there are some problems and deficiencies in the management mechanism, which also led to no "institutional" protection of the internal security management.

Internal security management mechanism cannot be effectively implemented. The enterprise lacks effective implementation mechanism of the management system. As a result, the management system is not implemented, and many management systems are still only on the surface.

4) Lack of Intranet security solutions. The lack of internal network security systems and programs has brought some obstacles on the intranet security management:

Most security systems are only from external intrusion. According to the intrusion from the outside, it has a large number of mature security systems to prevent, but the internal security threats and risks have rarely been noticed, or have noticed. Whereas, there is no perfect security system and security scheme to solve the internal security problems of enterprises.

Internal security system is not mature enough. In a small number of internal security systems, most of them just focus on a specific access, such as dial-up connection control and file protection. It is

simply a product in the technical sense, which cannot put forward the comprehensive scheme for internal security management.

2.3. Mobile GIS information security

As the mobile network is a combination of mobile communication network and technology, the information security includes hardware and software problems [6]. First of all, we start from the form of internal LAN of mobile communication to analyze the problem of network security. Secondly, from the point of view of security of the data itself, we analyze data security issues.

2.3.1. Composition of mobile GIS network The mobile is mainly composed of wireless communication network, mobile terminal equipment, geographic application server, and spatial database, as shown in Figure 1.

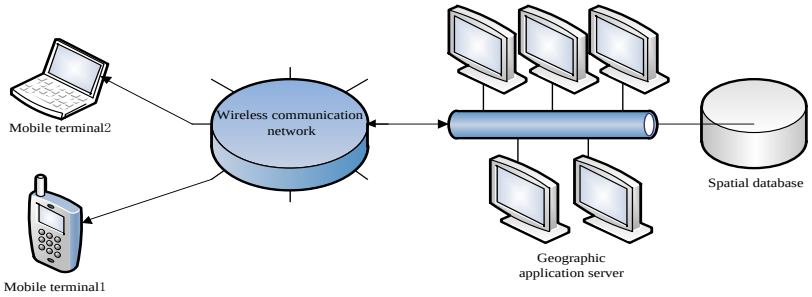

Figure 1. Composition of mobile GIS

Wireless communication networks: GSM, GPRS, and CDMA based on cellular communication systems.

Mobile terminal equipment: portable computers, PDA, WAP mobile phones, handheld GPS machines, including the display, RAM, high-speed processor and other components.

Geographic application server is the key part of the whole mobile GIS, and it is the GIS engine of the system. It is located in a fixed place, offering a wide range of geographic services and potential spatial analysis and query service for mobile GIS users. It has the following characteristics: to provide high quality maps, data and spatial query and analysis services; to handle a large number of service requests and uninterrupted access requests; to deal with the application request of huge data sets and a large amount of data; to increase the processing capacity without interrupting the operation; to be extensible, so as to adapt to the increase of data amount and access of new equipment; and uninterrupted feature of geographic service.

The spatial database is used to organize and store the spatial data related to geographic spatial data and corresponding attribute description information. It is the data storage center of mobile GIS, and it is able to manage the data, to provide a variety of spatial location data for the mobile application. It the data source for the geographic application server to realize geographic information service [7]. Mobile spatial database, in mobile GIS, plays the role of a data pump. It can make mobile devices interact with a variety of data sources, shield the difference of fixed network environment, and optimize the query conditions, so the entire mobile GIS has good flexibility and adaptability.

2.3.2. Information security problem of mobile GIS Because the mobile GIS independently exists not separates from the computer and network system, it also has a series of security problems, such as database security, data secrecy and so on. It mainly includes the following aspects:

Security and confidentiality of data transmission. The main contents include the determination of the security target, the encryption methods and algorithms in the network transmission, and the security level.

Security and confidentiality of data access, including for the different levels of users, through the different operating authorities, to achieve data access restrictions; for the different categories of data, to set different access rights; to establish operation log files for tracking the system operation; to encrypt the data and ensure the data security through the data dump, data backup and recovery.
The physical security design of the system is mainly to meet the technical safety requirements and safety requirements of equipment [8].

Personnel security. It is mainly to regulate the security and confidentiality of institutions and personnel, to determine the appropriate authorities and management practices, to develop contingency plans and a variety of safety rules and regulations, while to strengthen the safety awareness education.
In addition, it is necessary to have the ability to defend the virus, and deploy anti-attack device firewall and real-time monitoring system.

3. Mobile GIS enterprise information security architecture

From a technical point of view, a complete network security system should be three-dimensional. Different levels reflect the different security issues. According to the structure of the network and the application of network, it can be divided into the physical layer security, system layer security, network layer security, application layer security and security management. It is an effective way to realize the network and information security system through the good coordination between the technique aspect and management aspect [9]. Among them, the information security technology is achieved through the adoption of host computer system and safe network system containing the construction security, and equipped with appropriate security products. In the management level, it is realized through the framework of information security management system, as shown in Figure 2.

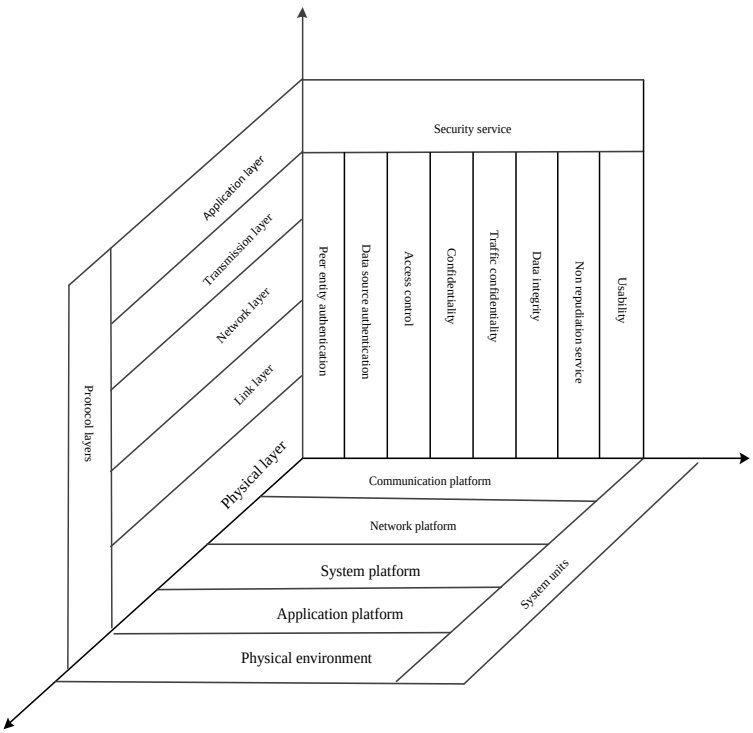

Figure 2. Three dimensional security technology framework

3.1. System layer security

3.1.1. Reasons for operating system vulnerabilities Programmers' human factors, in the process of programming, in order to achieve ulterior purpose, preserve the back door in the hidden place of the program code.

Restricted by the programmer's ability, experience and security technology at that time, in the process, there will inevitably be inadequate, and it will affect the efficiency of the program, but also lead to the authority enhancement of unauthorized users.

Due to the hardware, the programmers cannot make up for the vulnerability of the hardware, so the problem of hardware is reflected through the software.

Of course, everything is not perfect. As the desktop operating system - Windows is also in this way. And because of its monopoly in the desktop operating system, the problems will soon be exposed. In addition, compared with the operating systems of Linux and other open source code, Windows is a black box operation that ordinary users cannot get the source code [10]. As a result, the security issues are resolved by Microsoft itself.

3.1.2. Corresponding security measurements Install the latest version and patch program of the operating system in time. There will always be a number of system vulnerabilities being found. Usually, the software vendors will release a new version or patch program to patch security vulnerabilities, so as to maintain the used latest version can make the security threat minimal. Make the necessary security configuration. In the system configuration, close the services with security risks and unnecessary services, such as FTP, Telnet, finger, login, shell, BOOTP, TFTP and so on [11]. All of these protocols have security risks. Prohibit certain r orders, such as rlogin, rsh and so on. Strengthen the authentication in login process, set up a complex and not easy to guess password, carefully protect the account password and often change, prevent unauthorized users to easily guess the password, ensure the legitimacy of users, and restrict unauthorized access to the host. Strictly restrict the use permission of key documents in the system as follows, /.rhost, etc/host, shadow, group and so on, and strictly control the logged in visitor's operating authority, and limit the completion operation to the minimum range. Make full use of the log function of the system itself, record all the accesses of users, and regularly check the system security log and system state for early detection of possible illegal intrusion behaviors in the system, so as to provide the basis for decision-making for administrators and provide the basis for post review.

3.2. Security management

3.2.1. Security risks of management Management is an important part of network security. The imperfection of safety management system is one of the important sources of network risk. Security vulnerabilities caused by the network administrator, improper allocation or not in time upgrading of operating system and network application patch program, weak user passwords, freely using software downloaded by ordinary web site, setting up dial-up server inside the firewall but no authentication of the account, not strong user security awareness and so on, these management problems cannot be solved no matter how sophisticated the security strategy and security system are, and the network will be in danger.

3.2.2. Security measurements Information security technology is an important attribute of information security. The purpose of secrecy is to prevent the confidential information in the information system intercepted by the enemy. Encryption is an important means to realize the confidentiality of information. The so-called encryption is the use of mathematical methods to transform the message so that it is difficult for anyone else, in addition to the legitimate receiver, wants to restore the original message [12]. The process of converting cipher text into plaintext is called decryption. It can be seen

that encryption technology can make some important data stored on an insecure computer or an insecure channel without leakage.

Information authentication technology: information authentication is another important attribute of information security. The purpose of certification contains three aspects. The first one is to verify whether the information sender is real. The second is to verify the integrity of information, that is to say, to verify that the authentication information has not been tampered with, replayed or delayed in the transmission or storage process. The last one is to verify the non-repudiation of information, that is, to prevent the communication party denying having participated in an activity afterwards. Authentication is one of the most important techniques to prevent the adversary from making an attack on the system and falsification of information. The commonly used identification methods have access to the word and the way of holding, digital signatures and so on.

4. Conclusion

With the development of computer hardware and software, continuous improvement of network technology, and mobile devices with faster information transmission, the mobile terminal can browse a large number of multimedia contents. This paper analyzes the mobile compositions. In the paper, the security planning and solutions of the whole network are analyzed. In addition, for security threats that may occur, the corresponding solutions and security measures are deployed. More importantly, the framework for information security is constructed, which provides basis for the follow-up researches on the mobile GIS information security.

References

[1] Mai, B., Parsons, T., Prybutok, V., & Namuduri, K. (2017). Neuroscience Foundations for Human Decision Making in Information Security: A General Framework and Experiment Design. In Information Systems and Neuroscience (pp. 91-98). Springer International Publishing.

[2] Vithanwattana, N., Mapp, G., & George, C. (2016, September). mHealth-Investigating an Information Security Framework for mHealth Data: Challenges and Possible Solutions. In Intelligent Environments (IE), 2016 12th International Conference on (pp. 258-261). IEEE.

[3] Tupia, M., Bruzza, M., & Rodriguez, F. (2016, September). An information security framework for ubiquitous services in e-government structures: a peruvian local government experience. In Computer Science and Information Systems (FedCSIS), 2016 Federated Conference on (pp. 1309-1316). IEEE.

[4] Lee, J., Yoo, B., Lee, H., Cha, G. D., Lee, H. S., Cho, Y., ... & Kang, M. (2017). Ultra‐Wideband Multi‐Dye‐Sensitized Upconverting Nanoparticles for Information Security Application. Advanced Materials, 29(1).

[5] Bansal, G., Hodorff, K., & Marshall, K. (2016). Moral Beliefs and Organizational Information Security Policy Compliance: The Role of Gender. Proceedings of the Eleventh Midwest United States Association for Information Systems, 1-6.

[6] Kearney, W. D., Kearney, W. D., Kruger, H. A., & Kruger, H. A. (2016). Theorising on risk homeostasis in the context of information security behaviour. Information & Computer Security, 24(5), 496-513.

[7] Tsai, N., & Xiong, Y. (2016). An investigation of the information system security issues in Taiwan. International Journal of Business Information Systems, 21(3), 309-320.

[8] Zhou, C., Guo, Y., Huang, W., Jiang, H., Li, B., & Chen, J. (2016). Information security defense method of electric power control system based on digital watermark. system, 2, 4.

[9] Hameed, M. A., & Arachchilage, N. A. G. (2016). A Model for the Adoption Process of Information System Security Innovations in Organisations: A Theoretical Perspective. arXiv preprint arXiv:1609.07911.

[10] Lakhno, V. A., Petrov, O. S., Hrabariev, A. V., Ivanchenko, Y. V., & Beketova, G. S. (2016). Improving of information transport security under the conditions of destructive influence on

the information-communication system. Journal of theoretical and applied information technology, 89(2), 352.

[11] Fenz, S. (2016). researcher at Vienna University of Technology and SBA Research, an Austrian research center for information security, and founder of Xylem Technologies GmbH, a company supporting SMEs in identifying optimal information security strategies. From 2012 to 2015, Stefan was an appointed member of the European. Understanding Complex Urban Systems: Integrating Multidisciplinary Data in Urban Models, 129.

[12] Joo, J., & Hovav, A. (2016). The influence of information security on the adoption of web-based integrated information systems: an e-government study in Peru. Information Technology for Development, 22(1), 94-116.