SHS Web of Conferences **25**, 02010 (2016) DOI: 10.1051/shsconf/20162502010
ICITCE 2015

Research on network information security model and system construction

Haijun Wang
Department of Scientific Research, Shandong University of Political Science and Law, Jinan, Shandong, China

ABSTRACT: It briefly describes the impact of large data era on China's network policy, but also brings more opportunities and challenges to the network information security. This paper reviews for the internationally accepted basic model and characteristics of network information security, and analyses the characteristics of network information security and their relationship. On the basis of the NIST security model, this paper describes three security control schemes in safety management model and the relationship between the security service and security mechanism in the network information security architecture. On this basis, a network information security system model is proposed, which is composed of three parts, namely, the core layer, the logic layer and the implementation layer. Finally, this paper points out that the network information security protection technology is important, but it is still indispensable that management is in place.

Keywords: network information security model; core layer; logic layer; implementation layer

1 INTRODUCTION

Xi Jinping, the chairman of China who personally served as the central network security and information technology leadership team leader, has not only aired his views and opinions about the development of the internet, but also promoted the network to the national development and security level. Network security and information technology affect the country's security and stability, and the concept "Internet +" which is put forward shows the determination of China to transform the network big into the network power. We must have our own core technology to build network power and the construction of information security management system in the era of big data. Of course, we also should not do it without the protection of the law. "Strengthen the legislation of internet field, improve the laws and regulations about the service of network information, the protection of network security, the management of network social and other aspects, and regulate the network behaviour according to law."①

There is no uniform understanding toward the definition of Big Data [1], which is defined by Research organization Gartner as: The information assets need new processing mode to have the greater decision-making power, insight discovery and process optimization of massive, high growth rate and diversification. From the data category, the big data refers to the information which can't be dealt with by using traditional processes or tools. The definition of big data is defined by Wikipedia as: A collection of data can't be captured, managed, and processed with conventional software tools in the affordable time range. Big data has four features: Volume, Velocity, Variety and Value.② The features of big data are also reflected in two aspects, one is the data volume that grows in a geometric level, and the other is that the data source is very abundant. The proportion of non-structured data increases more and more. The security industry has begun to shift to the cloud with the widespread big data and cloud services, because the traditional security system, which can't effectively and quickly find unknown threats, has been very weak or disintegrated to the role of big data and cloud platform.

In general, security is defined as: "To avoid the nature or condition of danger" [1]. To maintain this nature or state, a variety of security policies are re-

①< Decision of the CPC Central Committee on major issues concerning comprehensively promoting the rule of law >

②Definition and nature are from the network: Baidu Know.

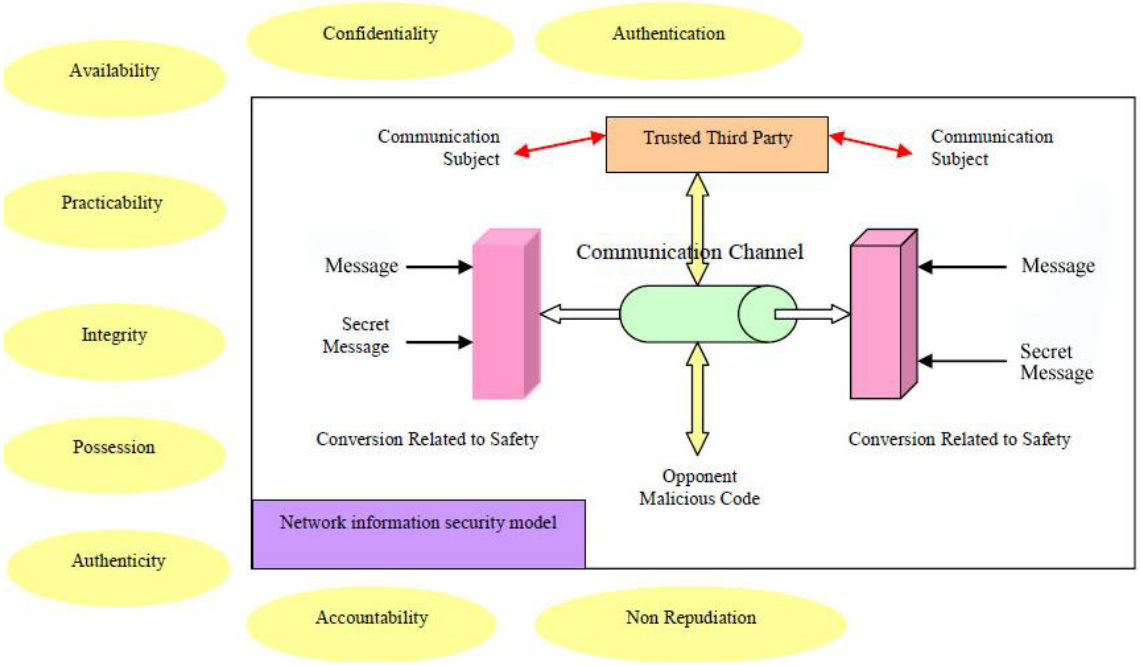

Figure 1. Basic model and characteristics of network security

quired. The scope and methods of each strategy are different. They cooperate with each other to form a security system to realize information security. A survey report pointed out that there are 42.8 billion network attacks that are monitored by all industries in the world in 2014, and the security problem is very serious. To build a network security system is the subject of the whole society. It not only needs the participation of all Internet users, but needs the network security enterprise with independent intellectual property rights and core technology. At the same time, the government should pay attention to the enterprise and give them policy and funding support. With the advent of the era of big data, the network information security is more complex and more difficult to defend [2].

2 NETWORK INFORMATION SECURITY MODEL AND CHARACTERISTICS

Network information security is a research field of many subjects including computer science, network technology, communication technology, cryptography, mathematics, information theory and so on [3]. It is a complex and difficult work to protect the information security of the network, because information is spread in the open network. Under the joint efforts of network security experts and researchers, the evaluation system of network information security is established to ensure that the characteristics of network information can play a role in normal. Network information security assessment is based on the nature and meets the conditions of security. It is considered that the network information is safe when it meets confidentiality, integrity, availability, accountability, authentication, non-repudiation and authenticity of the network information in dynamic and static processes①. Later, computer security experts of the United States have added two natures, namely, practicability and possession, which make the network security evaluation more scientific and reasonable. The network information security model [4] and characteristics are shown in Figure 1. The opponent or malicious code accesses the information through the communication channel from the client. Access will be subject to security checks such as a firewall and then will be confirmed by computer resources, data, processes, software and so on when they come into the interior and are authorized by trusted third party. All of this is to ensure the legitimate access and data security. The outermost ellipses of the graph are nine characteristics of the network information security.

Confidentiality refers to the characteristic that network information will not be disclosed to unauthorized individuals, entity or process, and it will not be used by the third party. Integrity means the information will not modified or damaged during storage or transmission, and the information packets will not be lost, disordered and so on. Information can't be modified by unauthorized third party to ensure the accuracy and completeness of the information and processing method. Availability is the characteristic of the information which is accessible and used when the authorized party is required, including the available and operable information of the static information and the visibility of the dynamic information content. The characteristic of the accountability is to make sure that

① Baidu Encyclopedia

the behaviour of an entity is uniquely tracked to the entity. The characteristic of the authentication is that the authorized party can identify and determine the authenticity of the information. The characteristic of non-repudiation is that it can demonstrate the ability of an act or event which has occurred, and it can't deny the act or event in the later. Authenticity, which mainly refers to the identity of the owner or the sender's identity, and applies to the entities such as users, processes, systems, and information and so on, is the credibility of the information. Practicability is a feature that describes the information encryption key is not lost. The information which lost the key cannot be decryption and lose the practicality. Possession means that the information carrier (such as the node and disk of the storage information) is stolen and lost the right of information.

3 CONSTRUCTION OF NETWORK INFORMATION SECURITY SYSTEM

To ensure the security of network information requires a multi-discipline knowledge and a common component of multiple security units. Each security unit as an individual has the integrity, and each security unit is combined to form a security system. In 1989, National Institute of standards and technology (NIST) in *Guidelines for the implementation of information resources protection* of *Special Publication SP500169* put forward: "The success of information resources protection project depends on the strategy used, and it also depends on the management layer to protect the information in the automatic system. As a policy maker, it should set the tone and emphasize the important role of information security in the institution. The main responsibility for the development of the body is to develop information resources security strategy to achieve the following objectives: reduce the risk and be in compliance with laws and regulations; ensure the continuity of the organization's operations, information integrity and confidentiality."[2]

3.1 *Model of security management and architecture of security system*

In the era of big data, network information security is characterized by diversification. To build a secure network system needs to develop a security plan at first and then needs a management model to implement and maintain security plans. At present, both of Federal agency and international organization have the good reference model about safety management model. British standard 7799 (BS7799) respectively explained the different areas of safety management practices. NIST [5, 6] security model has been widely examined by government and industry experts. [7] The hybrid security management model refers to the existing model and describes the security control plan with three parts as follows:

- Management control: security content which is formulated and implemented by management. The content includes process management, network security plan, network life cycle, risk assessment, prevention and control mechanism, and access to legitimacy and so on.
- Operation control: security of network operation by internal staff. The content includes emergency measures, personnel safety training, physical equipment security, software and hardware system maintenance control and the network information integrity.
- Technical control: technical measures to ensure the security of network information. The content includes logic access control, identity recognition, digital authentication, firewall, active defence, intrusion detection and so on.

Security management model, as the Internet reference model OSI, is a system framework for the department to use as reference according to the need. Agencies refer to the model to develop their own security policies and measures and establish a security management system which suits for the specific network according to their specific security plan.

In order to establish the security system, we should analyse the existing security control strategies and measures at first, find out other necessary security controls and form a security framework according to the requirements of safety management. The ISO7498-2 security architecture① is shown in Figure 2, it is the architecture of the open system interconnection model and the reference model of the network security system [8].

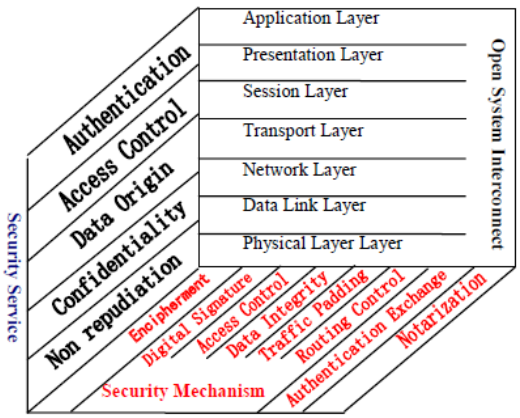

Figure 2. International standard ISO7498-2 security architecture

Using a three-dimensional form to describe the network information security reflects the relationship between the OSI reference model, security services and security mechanisms [9]. Security services are built on the security mechanism, and the relationship [3]

① International standard 7498-2: ISO 1989 (E)

between them is shown in Table 1-1 and Table 1-2. The relationship between security services and security mechanisms is more and more. A security service is guaranteed by a number of security mechanisms, and a security mechanism can achieve different security services vice versa.

Table 1-1. Relationship between security services and security mechanisms

Mechanism / Service	Encipherment	Digital Signature	Access Control	Data Integrity
Authentication	√	√	×	×
Access Control	×	×	√	×
Data Origin	√	√	×	√
Confidentiality	√	×	×	×
Non repudiation	×	√	×	√

Table 1-2. Relationship between security services and security mechanisms

Mechanism / Service	Traffic Padding	Routing Control	Authentication Exchange	Notarization
Authentication	√	×	×	×
Access Control	×	×	×	×
Data Origin	×	×	×	×
Confidentiality	×	×	×	×
Non repudiation	×	×	×	√

According to the requirement of OSI network reference model, the model constructs a security framework from two aspects, including network security services and network security mechanism. The former ensure data security from five aspects of service, and the latter involves eight kinds of security control mechanisms. Security mechanism mainly refers to the specific security technology or software which provides security services. There are two types of general security mechanism and special security mechanism. But with the development and progress of the hacker technology, the model has not been defined and standardized in DOS attack, intrusion detection and authorization management and so on.

3.2 *Build three-layer network information security system*

According to the security management model and security architecture, we carry out the risk assessment due to the business needs, a detailed understanding of the current network information security threats as well as the attack means of network information security. The three-layer network information security system is shown in Figure 3 which is built from the following aspects: Core Layer, Logic Layer and Implementation Layer.

Core layer. Network security policy is not only the core, but also the foundation. In this layer, its work is to analyse all kinds of basic information, develop safety standards, strategies and tactics, and make a unified plan for the security system. The content of the plan is generally: analyze the business needs of network and the operating environment of network; assess the security risk; assess equipment vulnerability, IT assets and network architecture, application system risk, data flow and physical layer risk and so on in accordance with international standards and assessment indicators and basic principles; form the security risk assessment report of network; develop a variety of safety standards and regulations; detail security requirements ; form a series of safety technical guidance, safety operation manual, work flow and specific implementation details. In short, the core layer is the development of strategic planning and standards, and it is the fundamental network information security system.

Logic layer. The logic layer is the mapping from the core layer to realize layer, collect and analyse the core layer of the planning. What's more, it provides a logical support for the implementation layer and makes the logic independent between the core layer and the realization layer, and it's easy to adjust and upgrade the security system. This layer is logically divided into two parts. One is the security technology system, which detailed statistical network attack technology and the way, corresponding to what defence strategy should be taken and implement the solution; the other is the safety management system standard, which establishes a variety of specifications according to the international standard and forms the management documents. Besides, it keeps physical access control, facilities and fire safety well and safeguards feasible resource protection and network access security from technical support. The safety protection technology is the application of the standard of safety management system and a part of the implementation. In fact, it is the complement and perfection of the system standard.

Implementation layer. It is the logical layer of technology implementation. It specifically achieves the network security from the specific operations, security management, defence technology, network physical equipment, personnel management and document management, including the security of data, communication, platform, application system, equipment operation, entities and so on. At present, there is a kind of relatively mature defence technology for

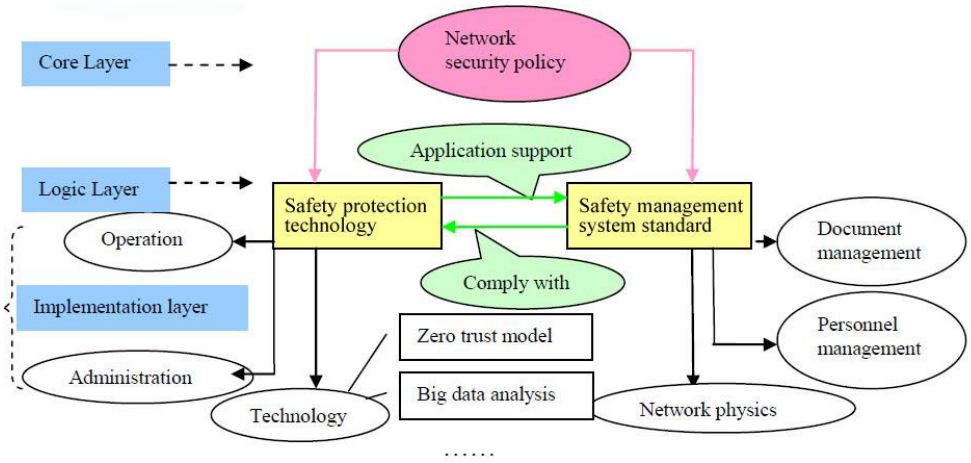

Figure 3. Three-layer model of network information security system

passive attack and active attack means, such as network access control mechanism, encryption mechanism and digital signature mechanism and so on. For personnel management, operating authority should be reasonably divided and distributed for internal staff. Migrant workers and users themselves must do self-protection and manage the security protocol. It should have strict procedures when staffs leave their post. From the institutional aspects, it should be strict with the post assessment management and train the safety awareness of the personnel regularly. Enterprises should strengthen and implement the responsibility system, ensure that workers should carry out the work within the prescribed limits of authority and bear the corresponding responsibility for the operation. At the same time, the information should be monitored to avoid being leaked intentionally or unintentionally by workers.

The network information documents should be strictly registered classified and managed according to the classification. Invalid file should be destroyed timely, especially when the electronic documents security risks are greater. Protection is also more difficult than it is mentioned in this paper, so the measures should be diversified. In order to ensure the authenticity of the document, data must be backed up regularly to prevent accidents.

"Zero trust security model" is a kind of protective measures due to the cloud security. It requires monitoring all aspects and follows the principle of "minimum authority" [5-7], including data encryption, key management and data ownership control and so on. So the concept of "zero trust network" appears. It's a solution to security problems, in which network boundaries are increasingly blurred and identification is more difficulty. In the "zero trust security model", any devices, ports and users are not trusted, and all must be in strict access control and security detection which causes a large amount of data that need analysis. In particular, the increase of unstructured data has brought great challenges to data analysis. The big data analysis technology comes into being, so the combination of big data, cloud computing data and security has become a trend.

3.3 *Management is the soul of security*

In the network security, whether from the use of the management model or the three-layer network information security system, the most important thing is the consistent management. Management is various, including data management, security management, regulatory management, document management, software and hardware system management, maintenance management and so on [8]. In the process of management, we must improve and modify the security policy and system, and apply it in practice, and continuously strengthen the security fortress. So management is the soul of network security.

In the process of security, we must strengthen the sense of responsibility for all levels of personnel and increase their awareness and understanding of information security through regular training. The advice of network information security providers, users or information security experts should be adopted. Through full preparation for the needs analysis and risk assessment of safety system design, the cost will be lower, and the efficiency will be higher. Combining the actual situation of network information security management, the following methods need to be done:

- Develop correct safety awareness. Everyone should be aware of their safety responsibilities and strengthen the training at regular time. Enterprises should regularly inform the network security situation.
- Establish the assessment system and the reward and punishment mechanism; strengthen supervision and inspection; protect the security system and measures to implement.
- Maintain the operation of the network in accordance with international standards, rules and regulations of the state and enterprises.
- For different levels of network, information and equipment, adopt different levels of security strategy.

4 CONCLUSION

The network information security is not only a technical problem, but also a management problem. Only by combining technical means and safety management, can we build an effective, safe and multi-level defence system. Building a network information security system does not mean that there is absolute security. And the network attack technology is also in continuous improvement and innovation, which encourage the development of network security management and technology. In the era of big data, the Internet information security is facing more threats, such as too much of the data leaking out seamlessly through the network, causing irreparable damage to us. Network security problems is a no easy task, the three-layer network security system construction technology may be a useful attempt in network security.

ACKNOWLEDGEMENT

This work was supported by grants from Shandong Social Science Planning and Management Office (13BGLJ11).

REFERENCES

[1] Xiang Heng & Fu Peng. 2005. *Information Security Management*, Chongqing: Chongqing University Press.
[2] Zhang Yunzhuang & Liu Jifeng. 2013. The opportunities and challenges for information security in the era of big data: An example of open information and intelligence. *National Defense Science & Technology*, 4(2): 6-9.
[3] Pan Minghui, *Principle and Application of Network Information Security Engineering*, Beijing: Tsinghua University press.
[4] Viktor Mayer-Schonberger & Kenneth Cukier. 2013. *Big Data: A Revolution that Will Transform How We Live, Work and Think*. Boston: Houghton Mifflin Harcourt.
[5] Introduction to industrial control networks, *IEEE Communications Surveys and Tutorials*, 2012.
[6] NIST Manufacturing Engineering. 2008. NIST Programs of the Manufacturing Engineering Laboratory, 03.
[7] Zhang Xuefeng. 2014. *Introduction to Information Security*, Beijing: People's Posts and Telecommunications Press.
[8] Information processing systems; Open Systems Interconnection; basis reference model; Part 2: Security architecture.
[9] Malek & Harmantzis F. 2004. Security Management of Web Services, Network Operations and Management Symposium, pp.175-189
[10] Charlie Kaufman. 1995. *Network Security*. PTR PrenticeHa.
[11] Cheswick B & Bllovin S. 1994. *Firewall and Internet Security*. Addison-Wesley.
[12] Xiao Junmo. 2003. *Network Information Security*. Beijing: China Machine Press, pp.222-256.
[13] Lemke, William A. Readshaw & Neil I. 2014. Coordinated network security management, International Business Machines Corporation, (12)
[14] Yang Haipeng, & Xu Zhiying. 2011. Network the study of constructing information security system. *Journal of Jilin Teachers Institute of Engineering and Technology*. (2):73-75.
[15] Malek & Harmantzis F. 2004. Security Management of Web Services, Network Operations and Management Symposium, pp.175-189
[16] Kim Jinpyo, Hsu Weichung, & Yew Penchung. 2007. COBRA: An adaptive runtime binary optimization framework for multithreaded applications. *IEEE Computer Society*, 40(9): 25225
[17] Lazer D, Pentland AS & Adamic L, et al. 2009. Computational social science. *Science*, 323(5915): 721-723.
[18] Kruger R. & Eloff J H P.A, 1997. Common criteria framework for the evaluation of information technology systems security. *Computers and Security*, 16(3): 207-207
[19] Kim Taesung & Kim Howon. 2006. Authorization Policy for Middleware in RFID System. IEEE.
[20] Wang Wenchao, & Haiming Shi, et al. 2013. National information security in the era of big data, *National Defense Science and technology*, (2): 1-5.