The Research and Exploration of Network Information Security

Yang lin[1,a]

1Department of Control Engineering, Naval Aeronautical and Astronautical University, Yantai Shandong 264001, China,

[a]email: liudi5388466@163.com,

Key words: Communication technology; Computer network; Information security; Confidentiality; Integrity;

Abstract: With the development of computer technology and communication technology, computer network will increasingly become important information exchange means, penetrated into every field of social life. Therefore, realizing the network vulnerability、potential threats and various security problems of the objective reality, taking strong security policy, encuring network information security, are the things that each country must face. In this paper, the basic information of the computer network application security issues and solutions are studied.

The Introduction

The coming of information society has brought opportunity for the global development. The use of information technology causes the transformation of production mode, life style and concept of the people. It promotes the development of human society and the progress of human civilization greatly. It brings people into a new era. The construction of information system has become the indispensable infrastructure of fields. Information becomes the important strategic resources、decision resources and control battlefield soul of society development.The informationization level has become the important symbol that measures a country's modernization level degree and comprehensive national strength. Preempting the information resource has become the important content of international competition. Country has promoted timely the national economy and social informatization, cleared the path of economic development in our country, endowed the new historical mission with information industry[1]. The construction and application of information network system must become the focus of national development in the new century. However, people are enjoying the benefits of network information at the same time, are also facing a severe test of information security. Information security becomes a realistic problem in the world, information security is closely related to national security.In the face of growing economic and information globalization trend, we should not only see it bringing us opportunities, at the same time, we should face up to the challenge caused by it. With the continuous development of computer network technology, the global information has become the trend of human development, computer network has gotten a number of applications in the field of national defense military, financial, business and daily life[2-3].

The research status at home and abroad

Access control technology is an important means of network data security protection.The static data security can be well ensured by the control over the means of user access to the data.The U.S. defense department has established two kinds of access control methods: independent access control policy and mandatory access control policy. Due to the complexity of application environment gradually, the two strategies on the control mode reveal great limitations. Password technology is the most powerful weapon to ensure data security[4-5]. The research of the password techniques has been the focus topic of research at home and abroad. Since 40s,it has not stopped the pace. International has come up with many kinds of cryptography,but more popular there are two major categories:one is based on the large integer factorization problem, the most typical representative is

the RSA; another kind is based on the discrete logarithm problem, the most typical representative is the Elgamal. Encryption technology and the study algorithm is relatively late in China, more famous is liu encryption algorithms, fully developed by the working group.Chinese scholars also proposed some password, and did some work in the rapid implementation of the password.Encryption technology is the core technology in information security technology, the critical national infrastructure could not have introduced or using someone else's encryption technology,can only be developed. Abroad not only leads domestic in the theory of password at present. Abroad are at the top in practical applications, formulated a series of password. At present, our country is still a gap with foreign in the application level of the password techniques. Therefore, we must have our own algorithms and standards to cope with the challenges of the future[6-7].

The basic concept of information security

Now, the information security has been known by the general public for various reasons.While it can't do household names, as reliance on computers and the internet increasingly, the factors that endanger the safety of information are increasing. The understanding and emphasis of information security gradually improve. Information security involves information confidentiality, integrity, availability, controllability. Comprehensive, it is to ensure the effectiveness of the electronic information. Information security is to make the information to avoid a series of threats, and ensure business continuity, minimize business losses, and maximize access to investment and business returns, involving information confidentiality, integrity, and availability. The information security is the concept advancing with the times[8]. It developed from the early communication security to pay attention to information confidentiality, integrity, availability of information security.and further development to today's information security and information security system, Simple confidentiality and static protection can not meet today's needs.Information security depends on the people, operations, and technology to achieve the organization's mission.The information technology infrastructure management activities also depends on these three factors,The steady state of information security means that the information security and policy, procedures, technology and mechanism can be implemented in the organization's information infrastructure. Data security concept of information is confidentiality, integrity, and availability.The user's safety concept is authentication, authorization, access control and based on the content of personal privacy, intellectual property protection. The combination of the two is the information security of security services, and these security issues will depend on the password, digital signature, authentication technology, firewall, disaster recovery.The password is the core of information security technology and management. The safety standards and system evaluation is the foundation of information security[9-10].Therefore, the information security refers to a country's state of social informatization from external threats and abuse.

The basic attributes of information security

The following basic properties: (1) information storage and transmission process is not broken.It do not delay, not random sequence and no missing data features. For military information, integrity damage causes delay. Damaging information integrity is the ultimate goal of information security attack; (2) availability:information can be legitimate users to access and can be used as requested order of characteristics.Availability attack is blocking the availability of information. Destroy the normal operation of the network and the relevant system is belong to this type of attack; (3) confidentiality: the information to unauthorized individuals, entities, or for the use of its characteristics.Military information security is particularly pay attention to information confidentiality; (4) the controllability: authority can control the confidentiality of information at any time.

Computer network threats

Computer network threats can be divided into two kinds: one is about the threat of network information; Second, the threat to the network equipment. There are many influence factors in computer network, there are some factors intentional, also be unintentionally.May be artificially, also may be unartificially; In the aggregate, network security threat mainly has three: (1) the human has no intention of mistakes. such as operator security vulnerabilities caused by wrong configuration, security awareness of user is not strong. The password of user chooses inadvertent,the own account optional of users shares with others and so on will pose threat to network security; (2) artificial malicious attacks. This is the biggest threats that computer network faces. The opponent's attack and computer crime belong to this category. Such attacks can be divided into the following two kinds: one kind is active attack, it destroys the validity and integrity of the information selectively in various ways. Another kind is passive attack, it obtains important confidential information by intercept and steals in normal working conditions. These two kinds of attacks can cause great harm to computer networks, and lead to the leakage of confidential data. (3) the network software vulnerabilities. Network software can't be one hundred percent without defects and loopholes, however, these loopholes and defects is the first target of the hacker attack, most of these events is incurred because security measures are not perfect. The important technology character of computer network is its various functions by using the technology to deal with.In fact, computer network equipment security and network information security is inseparable[11-12].

Ensure information security measures

Information security service refers to strengthen an organization's data processing system and information security. Security service's main purpose is to fight against attack, and ensure the basic attributes of information not be destroyed, at the same time, guarantee the information non-repudiation. Induces mainly contains the following aspects: (1) ensuring the confidentiality of information, information confidentiality is also called the confidentiality of the data. Some sensitive business information will not be illegal to steal, or even stolen, stealer cannot read information, such as: both parties to trade is not part of the third party to steal, the file is not illegal use of third party etc. Second, right of privacy, right of privacy is the problem that activities participants of computer network are concerned about.If the invasion of privacy problem is not solved, for users,it will be a very dangerous thing. (2) ensure the integrity of information, the integrity of information is the basis of network application. It contains two meanings: one is the authenticity of the data transmission, the information has not been tampered with in the process of network transmission,it is the true intentions of the sender that is consistent with the original information; The second is the unity of data transmission and data transmission mode can not arbitrarily change; (3) guarantee the non-repudiation of information, non-repudiation of information is also called the non-repudiation[13-14].

Conclusion

The computer network will become increasingly important means of information exchange, penetrated into every field of social life. Protecting the safety of network information is the thing that each country must face. This article tells the research background of the network information security, the basic concept and basic properties of information security, the threat of information security and the main content of information security services. The computer network information security problems and solutions are analysised, the common information security technology is introduced.

References

[1] Xun Yi，Yiming Ye．Security of Tzeng’S time-bound key assignment scheme for access control in a hierarchy．Knowledge and Data Engineering，IEEE Transactions on，Volume：15 Issue：4，July-Ang．2003．Page(s)：1054-1055．

[2]Joshi J．B．D．，Bertiono E．，6hafoor A．Hybrid role hierarchy for general ized temporal role based access control model．Computer Software and Applications Conference 2002. Proceedings 26th Annual International．2002．Page(s)：951-956

[3] Jason Crampton．Specifying and enforcing constraints in role-based access control．Proceedings of the eighth ACM symposium on Access control modelS and technologies．Como。Italy．June2-3．2003．Pages：43-50．

[4]Cungang Yang，Zhang C．N．Designing secure E-comerce with role—based access control．E-Commerce，2003．CEC2003．IEEE International Conference on，24—37 June 2003．Page(s)：313-319.

[5] Moyer M．J．，Abamad M．General ized role—based access contr01．Distributed Computing Systems，2001．21st International Conference on．．16—19 April 2001．Page(S)：391—398.

[6]Sandhu R．S．Coyne E．J．，Feinstein H．L．，Youman C．E． Role—based access control models．IEEE Computer，Volume：29，Issue：2．Feb 1996 Page(S)：37—47．

[7] W．J．Zhuang，M．Xie．Design and analysis of some fault—tolerance configurations based on a multipath principle(J]．Journal of Systems and Software，1994，25(1)：101-108．

[8]J．L．Marzo，E．Calle，C．Scoglio，T．Anjali．Qos online routing and mpls multilevel protection：A survey(J]．IEEE Communications Magazine，2003，41(10)：126_132．

[9] Tapolcai，P．H．Ho，A．Haque．Trop：A novel approximate link—state dissemination framework fordynamic survivable routing in mpls networks(J]．IEEE Transactions on Parallel and Distributed Systems，2008，l 9(3)：3 1 1-322．

[10]L．Li，M，M．Buddhikot，C．Chekuri，K．Guo．Routing bandwidth guaranteed paths with local restoration in label switched networks(J]．IEEE Journal on Selected Areas in Communications, 20Q5，23(2)l：437-449．

[11] P．J．Chuang．Cgin：a fault tolerant modified gamma interconnection network(J]．IEEE Transactions on Parallel and Distributed Systems，1996，7(12)：1301—1 306．

[12] Y．J．Suh，B．V．Dao，J．Duato，S．Yalamanchili．Software-based rerouting for fault-tolerant pipelined cornmunication[J]．IEEE Transactions on Parallel and Distributed Systems，2000，Il(3)：193-2n．

[13]M．Aggarwai，V．K．Sharma．Ant colony approach to constrained redundancy optimization in binary systems[J]．Applied Mathematical Modelling，2010，34(4)：992-1003．

[14] C．Jackson，A．Mosleh．Downwards inference：Bayesian analysis ofoverlapping higher-level data sets of complex binary—state on—demand systems[J]．Proceedings of the Institution of Mechanical Part Journal of Risk and Reliability，2012，226(2)：182-193．