THE STUDY ON NETWORK INFORMATION SECURITY

Muminov Sanjar Saidkulovich
Teacher of the Department, “Systematic and Practical Programming”, Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi, Uzbekistan

Shoraimov Husanboy Uktamboyevich
Assistant Teacher, Department “Systematic and Practical Programming”, Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi, Uzbekistan
Email id: khusan@shoraimov.uz,

Qudratov Shukrullo Abdiqunduz o'g'li
Student of the Department “Software engineering”, Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi, Uzbekistan
Email id: Shukrillo1998d@gmail.com,

ANNOTATION

The connectivity and openness of computer network greatly facilitates the sharing of resources. However, accompanied with the growing popularity and the expansion fields of network usage, unauthorized access, network data theft, hacker attacks, virus attacks and a series of network information security problems become visible. This paper focuses on the need of legislation protecting network information security, the existing regulations as well as the design principles of network information security system, and further explores the precautions on network information security.

Keywords: network information security, legislation, design principles preventive measures.

INTRODUCTION

The rapid development and wide use of the Internet has brought human beings into a brand-new information age. The Internet, which has greatly influenced and changed the way people live, permeates into politics, economy and the whole society. From government, enterprises, to any individual, the dependence on cyberspace is becoming more and more natural. The normal operation of the Internet is the guarantee of social order, and as a result, the security of Internet information becomes a very important issue. Especially since the "prism" Revelations, all governments take the network information security as a top priority.

In today's world of network information, a series of network information security events such as unauthorized access, destruction data integrity, jamming system operation, transmission virus via network ,line eavesdropping, illegal disclosure and use of personal information, and online fraud happen now and then. The following aspects from the business secrets and management, to personal privacy and property, and to national security and development are all violently threatened. Legislation to protect the safety of network information is imperative. Everybody is responsible for maintaining the security of the network information, and the action must be based on the law and the safeguard. Everyone shall have the right to use the

Internet, and at the same time should also be responsible for the corresponding obligations. In the network world, people should also adhere to moral and justice, and should not infringe other rights and interests, or disrupt the network simply for self-interest. Network legislation and civil rights are closely linked. With the strong pertinence, it is conducive to purify network environment for the positive role of the network. In effecting the radical cure of network problems, the overall system of information security mechanism should be established.

Security has become the bottleneck of the further development of China's e-commerce. Countries should strengthen the construction of network security to decrease black industry chain on the Internet and to safeguard network security. The system of electronic payment environment and infrastructure should also be improved to protect the safety and convenience of online trading .

The network information safety precautions involve technology, personnel, and management. The following focuses on technical aspects of preventive measures.

A. The Firewall Technology

Firewall technology refers to the isolation between local network and external network defense system. It sets up a security gateway between the Internet and Intranet to block the external network intrusion. It is to control the threshold of the communication from in and out of both sides.

Firewall is a very effective network security model of the Internet, through which risk area and safety area can be isolated from connection. Only the secure and verified information can be accessed into. Firewall technology is usually based on the packet filter technology, and the standard of packet filter is formulated on the basis of the security policy. Nowadays the main firewall includes packet filter firewall, proxy firewall and complex firewall. A complete set of firewall system is composed of shielding the router and proxy server. Packet filter firewall refers to packet filter or data grouping packet filter. The packet filter principle and technology can be thought of as the basis of various network firewall. Proxy firewall is the isolated point of Intranet and extranet, playing the role of monitoring and isolating from the communication flow of the application layer. Complex firewall is used together with packet filtering and proxy service.

The role of early firewall is in shielding the host and strengthening the control of accessing. However, the current firewall developed with the function of encryption, decryption, compression, decompression, and others. It increased the safety of network information.

B. Intrusion Detection Technology

Towards network intrusion, the intrusion detection technology is essential. Firewall just tries to resist the invaders. It is difficult to find intrusion attempts and successful invasion, but intrusion detection technology is effective to make up for the gaps. Network intrusion detection technology can detect the invasion behavior and invasion attempt, alerting the users in time to prevent intrusion behavior. Intrusion detection system type can be divided into host-based intrusion detection system, network-based intrusion detection system, and distributed intrusion detection system according to the source.

C. Data Encryption Technology

By using digital method to reorganize data, data encryption technology makes it unable for others except the legitimate vistors to restore the original information. Application of data encryption technology is the core of the network information security and the password means provide reliable guarantee. The digital signature and authentication based on password is one of the main methods to ensure the integrity of the information. The emergence of encryption technology guarantees for the global e-commerce, which makes it possible for electronic trading system based on Internet.

At present, the commonly used encryption technology are symmetric encryption and asymmetric encryption technology. Symmetric encryption is the conventional password-based technology,using a secret key for encryption and decryption. Asymmetric encryption does not use the same key for encryption and decryption. Encryption key is known to the public, called "public key"; the decryption key is known to the decryption people only, called "private key". The two keys must be matched to use. Perfect symmetric encryption and asymmetric encryption technology is still the mainstream of research in the 21st century.

D. Network Admission Control

Network admission control is one of the core strategies of network security and protection, including various control methods as the network access, permissions, directory and properties. One of the Network admission control is identity authentication. It is one kind of consistency validation, mainly including authentication basis, authentication system and safety requirements. Network entry is the first pass of the network access control, commonly through validating user account and password to control unauthorized access. User accounts and passwords should be strictly ruled, such as: password and account number should be long enough; numbers and letters (case-sensitive) or characters should be mixed; avoid using common digital password as birthday or ID number; The password should be as possible as complex and should regularly be updated to prevent to be stolen. At present, the commonly used identification technology is mainly based on “RADIUS”authentication, authorization and management (AAA) system. The second method of network admission control is access control. It rules a subject of some object with the operation of the power. Access control includes the type of data identification, access control, type control, personnel constraints and risk analysis. Access control and authentication technology are commonly used together, giving different operating authority to different identity of the users to achieve different security level of information classification management.

E. Virtual Private Network (VPN)

The function of virtual private network is: to establish dedicated network on the public network; to carry on encrypted communication. It is widely used in the enterprise network. VPN gateway functions basing on the packet encryption and the transformation of target address to realize remote access. VPN has a variety of classification, mainly classified according to the agreement, and can be realized through the server, hardware, software and so on. VPN sets up a special logical connection through the public network, allowing users to access to the internal network of different places with the same resources as local access without worrying about the problem of the leak.

F. Backup And Database Restoration

Network information security needs careful preparation. To put prevention first, users should get into the habit of backing up important data at any time and pay attention to the system running all the time. Database backup and recovery is the important operation for the database administrator to maintain data security and integrity. Backup is an effective way to restore the database, but recovery is to restore the original data after the accident by using the backup.

In addition to technical protection measures, the prevention from the aspect of personnel and management is also very important. Personnel should be trained for network information safety to prevent from computer crime and to raise the awareness of prevention. At the layer of management, a complete network information security management system needs to be established. The computer rooms, files, control, operation, and maintenance should be strictly divided for labor management.

CONCLUSION

Network information security is a complicated system engineering, involving the legislative protection, personnel, technology, equipment, management and other aspects of factors. The network information security system should be set as a whole. Network information safety is a combination of firewall technology, data encryption, and admission control to form a complete set of coordinated network security protection system. In addition to technology, we need to strengthen management, to improve the network information security legislation, to increase the intensity of law enforcement, and to formulate corresponding safety standards. With the above measures, network may serve human society in a better way.

REFERENCES

1) Daoyuan. Hu,Network Technology Tutorial. Beijing: Tsinghua University Press,2018.
2) Shibin. Zhang,Network Security Technology. Beijing: Tsinghua University Press,2018.
3) Tianjie. Cao, Computer System Security. Beijing:Higher Education Press, 2017.
4) Maozhi. Xu, Introduction to Information Security. Beijing:Posts and Telecom Press,2015.