2015 Seventh International Conference on Measuring Technology and Mechatronics Automation

Computer Network Security and Technology Research

Fan Yan1，Yang Jian-wen2，Cheng Lin1
(1. College of Math & Computer Science of Jiangxi Science & Technology Normal University, Jiangxi 330038, China)
(2. Chinese Unicom Jiangxi branch, Jiangxi 330000, China)
13970893711@163.com

***Abstract*—The rapid development of computer network system brings both a great convenience and new security threats for users. Network security problem generally includes network system security and data security. Specifically, it refers to the reliability of network system, confidentiality, integrity and availability of data information in the system. Network security problem exists through all the layers of the computer network, and the network security objective is to maintain the confidentiality, authenticity, integrity, dependability, availability and audit-ability of the network. This paper introduces the network security technologies mainly in detail, including authentication, data encryption technology, firewall technology, intrusion detection system (IDS), antivirus technology and virtual private network (VPN). Network security problem is related to every network user, so we should put a high value upon network security, try to prevent hostile attacks and ensure the network security.**

Keywords – Network Security; Authentication; Encryption; Firewall; Intrusion Detection System

I. INTRODUCTION

The rapid development of computer network, especially the emergence of the Internet, makes all kinds of information applications increasingly popular and widely spread. However, all kinds of information are transmitted and stored in the public communication network, which may be illegally wiretapped, intercepted, tampered or damaged by attackers with a variety of the purposes, thus resulting in an immeasurable loss. The treats on network security mainly display in: illegal access, pretending to be legal users, destroying data, listening in line and using network to transport virus, etc. With the network security problem increasingly prominent, whether the network security problem can be solved has become one of the key factors restricting the development of network. Network security problem generally includes network system security and data security. Network system security is to prevent the system from illegal attack, access and destruction; while data security is mainly to prevent confidential and sensitive data from being steal or illegal copied [1].

The computer network security problem is related to many fields, such as computer technology, communication technology, mathematics, cryptography, information theory, management and low. From the perspective of different fields, there are different solutions for network security problem, and these solutions should be integrated to solve the problem [2]. This paper mainly introduces network security background in Section 2 and network security technologies in Section 3, and Section 4 concludes the paper.

II. NETWORK SECURITY

A. Network Security Definition

The common nouns related to computer security are network security, information security, information system security, network information security, network information system security, computer system security, computer information system security, etc. These nouns imply ultimately the following two meanings: to ensure the safety operation of information system in the network environment, and to data stored, processed and transmitted in the information system are safely protected. In a word, "network security" in this paper refers to the reliability of network system, confidentiality, integrity and availability of information in the system, which is also the characteristic of network security [3].

ITU-TX.800 standard defines the network security logically from three aspects:

- Security Attack: refers to all the acts damage the information, including information denial service, message change, message replay, camouflage, traffic analysis, message release, etc.
- Security Mechanism: refers to mechanisms designed for detecting and preventing security attacks and for system recovery. It includes encryption, digital signature, access control, data integrity, authentication exchange, traffic padding, routing control, notarization and other mechanisms.
- Security Service: refers to the services to defend against the security attacks and improve the data process and information transmission security with one or more security mechanisms. It includes the peer entity authentication, data source authentication, access control, confidentiality, traffic flow confidentiality, data integrity, non-repudiation and availability, etc.

B. Network Security Architecture

Network security problem exists through all the layers of the computer network. According to the TCP/IP protocols actually run in the network system, Figure 1 shows the architecture of network security [4].

- Physical Layer Security: is mainly to prevent the damage, eavesdropping and attack on the physical path.
- Data Link Layer Security: ensures the data transferred through the network link from eavesdropping with techniques such as applies VLAN in LAN and encryption communication in WAN.
- Network Layer Security: ensures the network provides authorization services only for authorized users, thus

978-1-4673-7143-8/15 $31.00 © 2015 IEEE
DOI 10.1109/ICMTMA.2015.77

to guarantee the correct network routing and avoid eavesdropping or being blocked.

- Transport Layer Security: ensures the security of information flow.
- Operating System Security: refers to the security of operating system access control, such as database server, mail server, and Web server. Due to the complexity of operating system, multiple technologies are always applied to enhance the operating system security.
- Application System Security: the ultimate purpose of network system is to serve the users, so the application system security is also of great importance. It ensures the security with the security services provided by the application platform, such as communication content security, the both sides of communication authentication and the auditing system.

Application Layer	Application System	Application System Security
	Operating System	Operating System Security
Transport Layer		Transport Security
Network Layer		Security Routing/Access Control
Data Link Layer		Data Layer Security
Physical Layer		Physical Layer Information Security

Figure 1 Network Security Architecture

C. *Network Security Objective*

The objective of network security is to maintain the confidentiality, authenticity, integrity, dependability, availability and audit-ability.

- Confidentiality: the system only provides information for the authorized users.
- Authenticity: it can be guaranteed for the receiver that the information is from the claimed source.
- Integrity: the system only allows the authorized users to modify the information, thus to ensure the information is complete.
- Dependability: it prevents the sender or receiver from denying the transmitted or received messages.
- Availability: authorized users can get the required information resource services from the system.
- Audit-ability: it ensures all the activities in the system related to security can be reviewed.

III. Network Security Technologies

Technologies mainly applied in network security are authentication, data encryption technology, firewall technology, intrusion detection system (IDS), antivirus technology, virtual private network (VPN) and other technologies, in which authentication and encryption, firewall and IDS are the most important defensive lines of network security [5].

A. *Authentication Technology*

Authentication is to verify the authenticity of the entity and the legitimacy of information exchange. Authentication is based on cryptography, including identity authentication, message authentication, access authorization and digital identification [6].

(1) Identity Authentication

It recognizes the user identity by authentication, which is always before allowing users access to the network resources. “Username&password” is the most commonly applied method.

(2) Message Authentication

The both sides of communication confirm the communication content, to ensure that:

- The message is sent by the confirmed sender;
- The message is not modified in transmission;
- The message is sent to the expected receiver.

In order to guarantee the authenticity of the message source, private-keys of the both sides of communication can be applied to construct the message identification information, such as the shared private-key, K_s, and one-way Hash function, such as MD5 and Hash, which are often called as "data summary" and "data fingerprint". The data message sent by the sender contains data and data summary. After it is received, the receiver constructs new "data summary", and compares it with the former "data summary". If there's no difference between them, it implies that the information is not modified in the transmission.

(3) Access Authorization

Access authorization refers to confirm the user access authority to the information resources after identity authentication. Most systems process the access authority by adding access control list (ACL) after each resource.

(4) Digital Signatures

Digital signature is mainly to prevent the impostor, and to ensure that the receiver can prove the authenticity of the message received and the sender to a fair third-party (arbitration). At the same time, the signature must ensure that the sender can't deny its behavior, and also the receiver cannot deny or fake the received message.

Digital signatures technology is based on the encryption technology, which can be realized by symmetric-key encryption, asymmetric-key encryption and hybrid encryption algorithms. Assume n refers to the modes, d refers to the encryption key, and e refers to the decryption key. Open n and e to the public, keep d, and assume the encryption content as m, then the encryption process and decryption process can be described as:

$$\text{Encryption Process: } s = (m)\ d \bmod n \quad (1)$$

$$\text{Decryption Process: } m = (s)\ d \bmod n \quad (2)$$

B. *Data Encryption Technology*

As a kind of network security technology, data encryption technology is mainly to improve data confidentiality and prevent them from decoding. It generally applies two methods: symmetric-key encryption and asymmetric-key encryption [7].

(1) Symmetric-Key Encryption

Symmetric-key encryption is also called as private-key encryption or single-key encryption. It applies the same key to encrypt and decrypt the message, which is shared by both the sender and receiver. Symmetric-key encryption is simple and fast, thus has been widely used. The most popular algorithms are RC2, RC4, DES, 3DES, SKIPJACK, IDEA, CAST-128, etc. The most important problem in these algorithms is how to transmit the private-key securely to each other.

(2) Asymmetric-Key Encryption

Asymmetric-key encryption is also called as public-key encryption, which applies a public-key and a private-key. The message encrypted by the public-key can only be decrypted by the matching private-key. Asymmetric-key encryption is more complicated and secure, of which RSA is the most popular public-key encryption algorithm.

C. *Firewall Technology*

Firewall is a security system between the internal network and the external network, which is used to strengthen the access control between networks. It helps prevent the external users access to the resources in the internal network illegally, thus protecting the internal devices and data [8].

(1) Basic Functions of Firewall

- Filter the data packets pass through the network;
- Manage the access behaviors pass through the network;
- Plugging some forbidden access behaviors;
- Record the information content and activities pass through the firewall;
- Detect and alarm the network attacks.

(2) Key Techniques of Firewall

The main technologies applied in the firewall are: packet filtering technology, application gateway and proxy technology. These technologies can be used alone or in combination.

Packet filtering technology is based on the network layer, and acts on the IP layer, which is constructed by filtering router. It checks each arriving IP packet according to the security strategies, and determines whether to pass or block, thus to realize IP packet filtering. Its core is the secure strategy, namely the filtering algorithm design. The advantages of packet filtering technology are simple, fast, and transparent to the user and have little effect on the network performance. However, it is difficult to construct and manage the packet filtering rules, and it lacks auditing, tracking and verification functions.

Application gateway provides access control in the application layer. It checks the flow in detail, thus runs slower than the packet filtering firewall. Application gateway can hide the topology of the internal network, so it has effective auditing facilities to monitor the flow and process the log file. These files contain rich information, such as source and destination network address, user account, protocol type, access start and end time, and data transferred from different directions. As application gateway is complementary with the packet filtering, many current applied a new generation of hybrid firewall combining these two technologies [9].

Proxy technology acts on the application layer, which core is the proxy server process running on the firewall host. It completes the specific TCP/IP function instead of the network user, and every specific application has a corresponding program. The advantages of proxy technology is that it has strong data flow monitoring, filtering, recording and reporting function, which shields the internal network topology and strength the network security. However, the proxy service software of every network service has to be specifically designed and developed, which has to be completed on the special workstation.

D. *Intrusion Detection System*

Intrusion detection system is a kind of active network security technologies, which is a reasonable supplement of firewall. It collects information actively from the internal system and various network resources, and analyzes the possible network invasion or attack. Thus intrusion detection system extends the security management ability, including security auditing, monitoring, attack recognition and response, and improves the integrity of information security architecture [10].

Intrusion detection system has the following functions:

- Detect and analyze the user and system activity;
- Audit the system configuration and vulnerability;
- Identify the known attack patterns and report to the related people;
- Statistics and analysis of the abnormal behavior patterns;
- Evaluate the integrity of important systems and data;
- Manage the operating system, and identify the user behaviors violating the security strategies.

From the technology principles, intrusion detection technology can be divided into two types: anomaly detection and misuse detection.

(1) Anomaly Detection

Anomaly detection assumes that all the intrusion behaviors are different from normal behaviors. By establishing the normal behavior profile of the target system and its users, all the system states different from the normal behavior profile can be considered as suspicious. The anomaly threshold and feature selection is the key to anomaly detection technology. The popular algorithms applied include probabilistic method, predictive pattern generation and neural network method.

(2) Misuse Detection

Misuse detection assumes all the intrusion behaviors and means can be expressed as the same pattern or character, so all the known intrusions can be detected by matching method. The key of misuse detection is how to express the invasion pattern to distinguish the normal behaviors and invasion. The popular algorithms applied include expert system, pattern matching, model reasoning and state transition analysis.

IDS can be placed in the network hosts or network perimeter, such as between the firewall, around the Internet server, neighbor links, WAN backbone and server farms.

E. *Antivirus Technology*

The computer virus is commonly spread by three ways: removable storage media such as U disk; CDs and network. The prevention of virus should be paid special attention, and information from removable storage media must be checked carefully. Also, virus filtering software should be installed in the firewall, proxy server, SMTP server, network server and mail server. Users should update the virus database and check the disk in time. Prevent and kill virus is a long-term task, thus users should always enhance vigilance unremittingly for network security [11].

F. *Virtual Private Network (VPN)*

The private network realized by the public network is called as VPN. Specifically, VPN refers to a private network in the public network, in which data is transmitted through the virtual safe channel in the public network. VPN solves the problem of how to transport the internal network information in the Internet safely. VPN will develop into the main technology in enterprises in the future due to its advantages, such as remote access functions, less costs, strong expansibility, convenient management, overall control, and so on [12].

IV. Conclusions

We should look on the computer network technology problem dialectically. On one hand, the networking of information system provides the resources sharing and convenience for users. It improves the system efficiency and reliability through distributed processing, and also has good scalability. On the other hand, the following characteristics also make the information system unsecure. Thus, network security is the new challenge for the current computer network field, and will also be one of the most important researches in the future.

References

[1] C Bing, W Lisong. Research on Architecture of Network Security [J]. Computer Engineering and Applications, 2002, 38(7):138-140. DOI:10.3321/j.issn:1002-8331.2002.07.047.

[2] Marin G A. Network Security Basics [J]. Security & Privacy, IEEE, 2005, 3(6):68-72.

[3] Y Bingyu. An Elementary Introduction to Computer Network Security [J]. Computer Knowledge and Technology, 2009.

[4] X Deqin, Z Quan, Z Min, P Chunhua, Z Mingwu. Computer Network Principle and Applications [R]. Beijing: National Defense Industry Press, 2011, (2).

[5] S Siyuan, Z Shouyi, S Yaobin. On the Study and Trend of Network Security Technologies[J]. Journal of System Simulation, 2001,11(13).

[6] Q Yi. A Study on the Identification Authentication of Network Security [J]. Journal of Huaihai Institute of Technology, 2001.

[7] S Yongjie. Research on Communication Encryption Technology of Network Security [J]. Telecom Power Technology, 2014.

[8] L Dong, Y Peng. Network Security and Firewall Technology [C]. //proceedings of 2010 3rd International Conference on Computer and Electrical Engineering (ICCEE 2010 no.2). 2012.

[9] L Lun, Y Lan. School of Graduates, China University of Geosciences, Wuhan 430074. An Improved Application Gateway System [J]. Computer Engineering and Applications, 2003, 39(5).

[10] Ali Aydın M, Halim Zaim A, Gökhan Ceylan K. A Hybrid Intrusion Detection System Design for Computer Network Security [J]. Computers & Electrical Engineering, 2009, 35(3):517–526.

[11] W Xiaolin. Study on Computer Network Antivirus Mechanism based on Antivirus Software [J]. Network Security Technology & Application, 2014.

[12] L Chuiwei. On Virtual Private Network [J]. Journal of Huangshi Polytechnic College, 2005.