Network Media Communication System of the Security Technology

Chun-xu Zhang* · Yun-ho Shin**

ABSTRACT

There are multiple reasons that caused the present serious status of network security, including Internet itself having a weak basis. However security is usually discarded when it contends with performance. As the world becomes more tightly interconnected, security technology continues to mature, organizations are feeling a greater need to rediscover network security. Network security technology generally concentrates on protection of the network infrastructure and, by implication, the protection of the user. This is a paper, describe current problems of network security and propose solutions.

Keywords

Network Security, Security Devices, Firewalls, Intrusion Detection

Ⅰ. Introduction

The 21st century world computer all communication will unite the same place through Internet, the information security connotation has also had the radical change. It not only turned one kind of extremely ordinary guard from the general defense, moreover also turned the there is no place from one kind of special domain not in. Network security is the most important thing on the planet." We have heard these words uttered with great conviction many times. The reason is simple, and at one time it may have even been valid: Performance directly contributes to the bottom line while security provides only indirect benefits. The humanity marches into the 21st century this information communication society, network society's time, our country will establish a set of complete network securities system, specially will establish from the policy and the law has the characteristic the network security system[1].

II. Current Problems

The information security is an important question which the national development faces. Regarding this question, we have not considered it from the system plan, from the technology, the industry, the policy develops it. The government not only will be supposed to see the information security the development is an our country high tech industry part, moreover should see, the development security industry policy is an information communication security safeguard system important constituent, even should see it to our country future the electron, the information development will play the count for much role[1][2].

Poor security could let hackers obtain Internet users' Social Security and credit card numbers and otherwise compromise their privacy. This lack of security could promote identity theft, fraud, and other crimes. Network threats are increasing in complexity,

* Dept. of Electric Comm. Eng. Chonnam National University
** Dept. of Comm. Eng. Tennessee University
접수일자 : 2008. 01. 17
심사완료일자 : 2008. 02. 23

as demonstrated by the destructive distributed denial-of-service (DDoS) attacks on major Web sites and dangerous worms such CodeRed. Computer-security issues were the subject of a recent, the government must provide more funding and support to address the problem.

The massive surge of interest in the Internet, along with the emerging use of low-cost residential broadband networking for homes and small enterprises, has given rise to a concentrated study of network security practices[1]. The explosive growth of networking technology continues to redefine the rules for maintaining the privacy and integrity of electronic data[2][3]. There is a staggering amount of personal, commercial, governmental, and military information in the various networking infrastructures worldwide. This vast connectivity also poses monumental risks. Almost anyone can reach out to the network, which often means almost anyone can reach in. In short, network security is an issue that can no longer be postponed. Fortunately, security measures do not have to be expensive or complicated—a reality the networking community has only recently taken to heart. Network security itself, however, must be better understood and embraced, preferably before a compromise occurs.

III. Propose Solutions

3.1 Characteristics

A national information communication security system includes national in fact the laws and regulations and the policy, as well as technical and market development platform. Our country when constructs the information defense system, responds the strength to develop the oneself unique security product, our country must want truly to solve the network security problem, the final means are through the development nationality's security industry, leads our country network security technology the whole enhancement[4][5].

Below the network security product has several major characteristics: First, the network security originates from the security policy and the technical diversification, if uses one kind of unified technology and the strategy is also unsafe; Second, the network safety mechanism and the technology want the unceasing diastrophism; Third, along with the network in social aspect extending, enters the network the method more and more to be also many, therefore, the network security technology is an extremely complex systems engineering. Has the Chinese characteristic for this establishment the network security system, needs the national policy and the laws and regulations support and the group unites the research development. Safely with counter-safe likes the contradictory two aspects, always unceasingly upwardly climbs, therefore the security industry future also will be along with the industry which the new technological development but unceasingly will develop.

3.2 Establishing a Plan

A thread that spans most definitions of network security is the intent to consider the security of the network as a whole, rather than as an endpoint issue. A comprehensive network security plan must encompass all the elements that make up the network and provide five important services :

1) Access. Provides users with the means to transmit and receive data to and from any network resources with which they are authorized to communicate.
2) Confidentiality. Ensures that the information in the network remains private. This is typically accomplished through encryption[4].
3) Authentication. Ensures that the sender of a message is who he claims to be.
4) Integrity. Ensures that a message has not been

modified in transit.

5) Nonrepudiation. Ensures that the originator of the message cannot deny that he sent the message. This is useful for both commercial and legal reasons[6][7].

An effective plan is also built on a thorough understanding of security issues, including the potential attackers, the needed level of security, and the factors that make a network vulnerable to attack. This understanding helps you define the level of security that is appropriate for the information the network contains and the environment in which it operates.

3.3 Security Devices and Measures

Once you have shaped your network security plan, you can begin to incorporate the appropriate technology to provide a secure environment. Several items may be common to many plans, but not all the elements we describe here must be in place. What you use should be based on a thorough assessment of the risks present and your plan's objectives. Many security devices—from stand-alone products to protocols incorporated into network elements—have been developed[5]. The brief description of firewalls and intrusion detection we offer is only a sample of popular devices.

3.3.1 Firewalls

Firewalls enforce an access policy by operating as a gateway between two networks[6]. There are two major classes. Packet filter firewalls examine endpoint identifiers in datagrams passing through a link to determine if each packet should be allowed to proceed. For example, an IP packet filter can examine the source and destination IP addresses, the port being used, and the specified protocol field. Depending on the firewall's degree of sophistication, it might also maintain the state associated with each IP flow so that flows can be statistically analyzed.

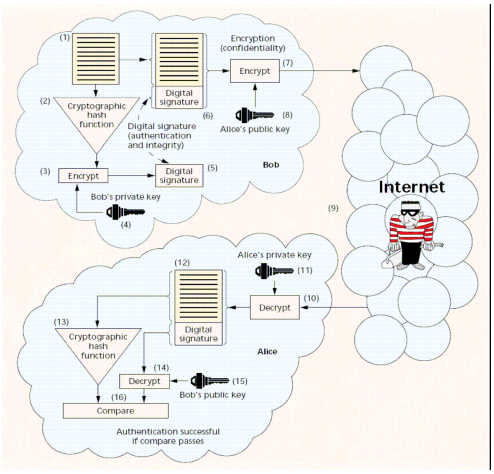

Fig. 1 How public key cryptography works.

3.3.2 Network intrusion detection

Network intrusion detection devices try to detect and call attention to odd and suspicious behavior. Anomaly detection devices use statistical methods to try to detect activity that deviates from normal behavior. These devices generate logs and alert system administrators when they detect suspicious activity. Misuse detection devices examine traffic and use patterns, and try to identify a pattern that they can compare to signatures or scenarios known to be dangerous or suspicious. These devices can be applied only against known attack patterns. In the same way popular virus checkers are updated with signatures used to check system memory and files, misuse detection devices must be periodically updated with new signatures as new attacks are detected and characterized.

IV. Conclusion

The problems and solutions for both internet and Web users are complex and still developing. Some of

the articles we've included describe current problems and propose solutions. Our capacity to protect information worldwide will grow only when more network owners begin to plan for and consider these complex issues. The articles in this issue are inte-nded to alert you to the risks and some solutions and to encourage you to develop and implement security methodologies and strategies before-rather than after-an incident.

References

[1] A. Rubin, D. Geer, and M. Ranum, "Web Security Sourcebook", John Wiley & Sons, NewYork, 1997.

[2] The ATM Forum Technical Committee, ATM Security Specification, Version 1.0.

[3] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", Internet Draft (work in progress, not the final standard, available from http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ipsec-arch-sec-05.txt).

[4] B. Schneier, Applied Cryptography, 2nd ed., "John Wiley & Sons", NewYork, 1996.

[5] S. Garfinkel and G. Spafford, "Practical UNIX and Internet Security", 2nd ed.,

[6] O'Reilly & Assoc., Sebastopol, Calif., 1996.

[7] D. Chapmon and E. Swicky, "Building Internet Firewalls", O'Reilly & Assoc., Sebastopol, Calif., 1995.

Authors

Chun-xu Zhang

Was born in Beijing, China, on May 13, 1984. She received the B.E degree from the Beijing Institute of Petro and Chemical in 2006, Beijing china, the M.S degree in the Electric Communication Engineering at Chonnam National University from March 2007 to now.

Email : xuxu0513@hotmail.com

Yun-ho Shin

Was born in Kang Rung, South Korea, on September 04, 1976. He received B.E degree in entered the Department of Mass Communication Science of Kyung-Nam University, 1995 Masan in Korea . The Department of Mass Communication science of Joong-Ang University, 2003. M.S. Seoul, Korea, the M.E. degree in enconomics from the state University of New-York at Buffalo. In 2007.(M.S. Completion), and degree in the Dept. of Communication and Information from the University of Tennessee of USA, from 2007 to 2008.(Postdoc.)

Awards : Mass Communication science.

Email : juwhan78@hanmail.net