Network Security for the Broadband Era

Makoto Kayashima
Yasuhiko Nagai
Masato Terada

OVERVIEW: The Internet is now an indispensable information infrastructure for organizations. The telecommunication infrastructure [e.g. ADSL (asymmetric digital subscriber line), cable TV, etc.] providing broadband network services offering multimedia data contents like movies and voice over the Internet has also become widespread. As a result, many important services are being provided on the Internet. At the same time, however, networks have experienced rapid increases in virus attacks and illegal accesses. Thus, broadband networks are in need of improved information security. "Security 3A," which stands for "Authentication," "Authorization," and "Administration," is a comprehensive approach to ensuring the security of broadband networks. It takes advantage of technologies such as encryption and authentication. Hitachi is currently engaged in the development of security 3A systems for the broadband era.

INTRODUCTION

BROADBAND networks are beginning to carry information of high asset value, such as multimedia contents. Consequently, the risks of virus attack or illegal access have been increasing. Thus, broadband networks are in need of improved information security.

"Security 3A," which stands for "Authentication," "Authorization," and "Administration," is a comprehensive approach to ensuring the security of broadband networks.

In this paper, we describe the roles of "Security 3A" in the broadband era and introduce Hitachi's approach to "Security 3A."

AUTHENTICATION

Authentication is a technology to identify an accessor. The general process for authentication is as follows:

(1) The authenticator checks the identifier (e.g. user name) of an accessor.

(2) The authenticator checks the authentication information (e.g. password) of the accessor by comparing it with the authentication information it has registered beforehand to identify the identifier. The authentication information should be able to be provided only by the accessor.

Organizations who manage their networks via the Internet take increased risk of illegal accesses such as the "replay attack" (i.e. pretense by means of authentication procedures illegally obtained via the network).

Authentication Method Using Cipher Technology

Cipher technology enables the authentication procedure to prevent replay attacks (see Fig. 1). The

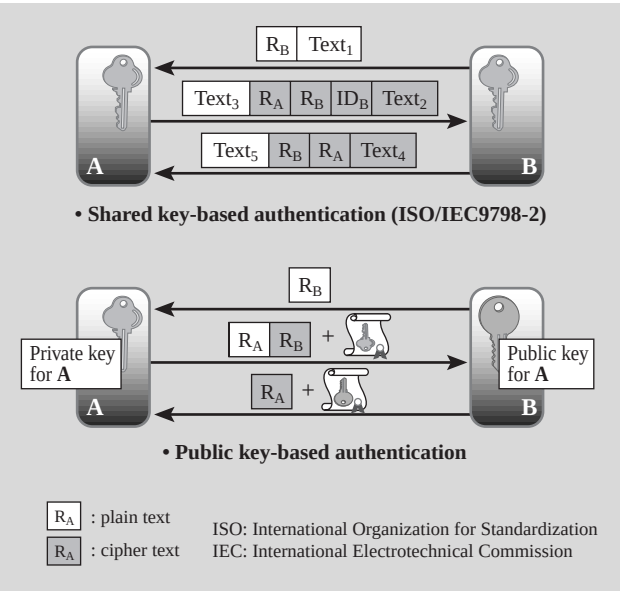

Fig. 1—Authentication Method Using Cipher Technology. With the shared-key or public-key cipher technology, it is possible to prevent the replay attack.

process of an authentication with cipher technology is as follows:
(1) The authenticator generates a random number and then sends it to the accessor.
(2) The accessor encrypts the random number with a shared key or a private key and sends it back to the authenticator.
(3) The authenticator decrypts the encrypted number with the shared key or a public key. If the received number is the same as the expected number, the authenticator identifies the accessor.

The authentication information is changed each time the accessor accesses the network by using random numbers generated by the authenticator. In this way replay attacks can be prevented.

The shared key-based authentication method has been standardized as ISO/IEC9798-2[1]. Hitachi provides VPN (virtual private network) products[2] employing this authentication method.

Content Authentication

The broadband era is characterized by various multimedia contents being sent and received via the Internet. As digital contents are easily copied, we consider that content authentication technologies are indispensable to assure proper use of contents. Hitachi is developing content authentication technologies that use electronic watermark technologies for static and/or moving images.

Human-crypto

Not only has the number of Internet users been increasing, users' computer competence has diversified. That is, users now tend to range from knowledgeable ones to inexperienced ones. Also increasing is the number of users who have little consciousness of security, and these people, in particular may inadvertently leak their authentication information. On this account, we consider that it is important to enable an accessor to conduct a simple and safe authentication by himself. Consequently, Hitachi has been developing an easy-to-use authentication technology, called human-crypto, which uses biometrics as authentication information. This technology improves the recognition precision of biometric data and allows acquisition of biometrics information without inconveniencing the user. Hitachi's efforts in this area stress a technology that is user-friendly and can improve the precision of authentication by combining multiple biometrics.

PKI (Public Key Infrastructure)

In the public-key authentication, we need to assure that a public key used by an accessor is not a fake one. The framework to guarantee the authenticity of public keys is called the Public Key Infrastructure, PKI, where a Certificate Authority, CA, issues public-key certificates. Large-scale systems like an electronic government require multiple CAs that issue public-key certificates. Therefore, a mechanism is needed that allows public-keys issued by different CAs to be authenticated by any CA. Hitachi is currently developing such a PKI for large-scale systems.

AUTHORIZATION

Authorization is a technology for limiting access to resources such as filing systems by using access permissions and information of accessors. The authorization is done by an operating system, and only authorized persons are permitted to write or read resources within the limits of the right authorized. In this section, we describe the threats to network authorization and introduce Hitachi's plan to deal with them.

Buffer Overflow Attack and its Countermeasure

The buffer overflow attack causes faulty software operations by an attacker inputting data with a longer buffer length than the maximum in the system's design. For example, if an attacker inputs to a web server data whose length is longer than the maximum buffer length and that also includes a program called "shell code," it may be possible for the attacker to access the server's resources like he or she were an authorized user. To prevent such a buffer overflow attack, it is important to use software that does not cause faulty operations, i.e., Buffer Overflow Free Software. However, it is difficult to design and develop network systems that can defeat a buffer overflow attack by using software only.

Consequently, Hitachi has been developing an authorization enhancement tool to minimize the damage from faulty software operations (see Fig. 2). This tool's access control function can accept or deny access based on not only the accessor's identity, but also the programs used for access. Thus, this access control function not only accepts or denies accesses based on accessors but also denies unexpected accesses.

Cross-site Scripting Attack and its Countermeasure

The cross-site scripting attack was first identified

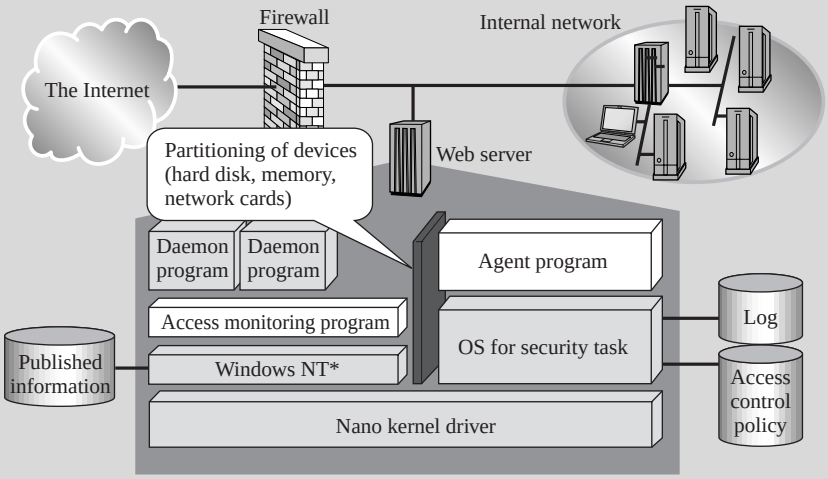

Fig. 2—Enhancement of Authorization Function.
The enhanced authorization tool provides the access control function that accepts or denies access based on not only accessors but also the program used for access.

in 2000. In this attack, an attacker sends to a target web server malicious contents with bad scripts enabling irregular processes. These bad scripts cause improper browser operations when an accessor uses the target web server. The cross-site scripting attack enables the attacker to access the internal data of accessors' PCs from the targeted web servers.

To prevent the cross-site scripting attack, we need to do the following:
(1) Never recklessly execute scripts downloaded from external web pages, i.e., always identify the scripts.
(2) Always check that the contents cause no trouble whenever you make them using a web server containing an external web page (data).

Hitachi has been collecting information on security, including cases of the cross-site scripting attack as well as countermeasures, and has developed checking tools for these cases. The information and tools are provided to system engineers who develop networks.

SECURITY MANAGEMENT

In the previous sections, we described the authentication and authorization technologies that are indispensable as base technologies to ensure network security in the broadband era. Recently in the limelight is security management technology that assures effective use of the base technologies as well as embeds them into systems. In this section, we describe the trend in standardization of security management and introduce Hitachi's activities in this field.

International Security Evaluation Standard

ISO15408

ISO15408 is the international security evaluation standard that regulates basic security functional requirements, quality assurance requirements, and assurance levels. In developing network products and network system designs for our products, we need to select security functions regulated by ISO15408 and to write a "Security Target," ST.

Hitachi has developed an Integrated Construction Method for ST to guarantee the uniformity and pertinence of the ST work and also provides a manual for developers and system engineers. This manual enables general developers or system engineers who are not experts in security analyses and evaluations to prepare STs efficiently.

International Operation Standard for Security Management: ISO17799

As an international operation standard for security management, ISO17799 is now being standardized based on British Standard 7799 (BS7799). ISO17799 sets the following requirements: An Information Security Management System (ISMS) needs to be established in order to establish a framework through definitive documentation of management objects and countermeasures and execute selected management objects and countermeasures.

Security Integrated Management Tool

It is expected that a variety of security equipment to authenticate and authorize hosts and contents will be used in the broadband network era. The equipment

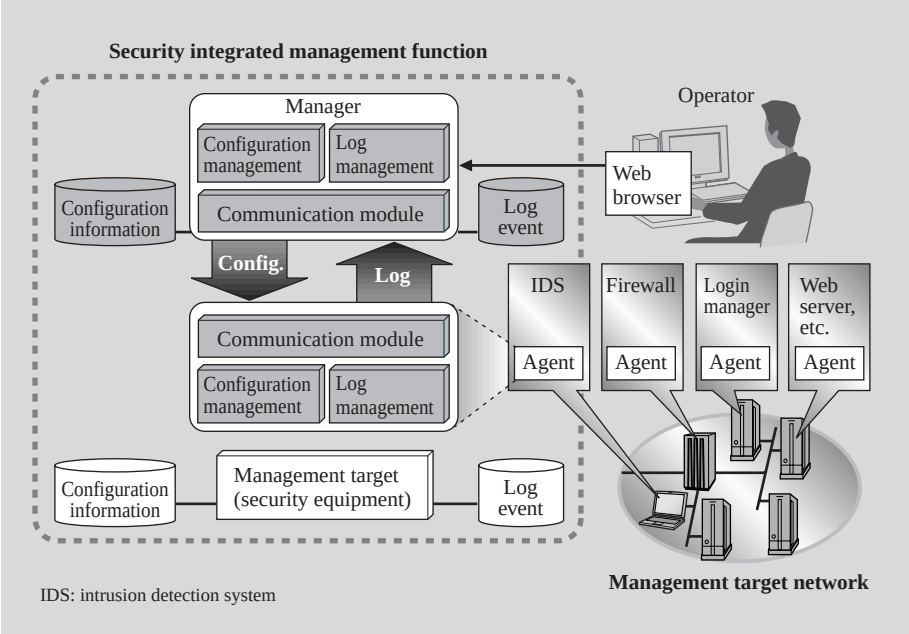

Fig. 3—Image of Security Integrated Management Function. The security integrated management function executes the integrated management including the configuration, log and event management of security tools.

will satisfy the security requirements regulated by ISO15408. However, a high level of skill is needed to use the equipment properly and manage the system operations based on ISO17799. Therefore, Hitachi is developing security integrated management functions that support the proper use of security tools. These functions realize the integrated frameworks for security management (see Fig. 3).

CONCLUSIONS

In this paper, we have discussed "Security 3A" technologies that are important for ensuring network security and introduced Hitachi's "Security 3A" activities. As network security will become more important in the IPv6-based broadband era, Hitachi intends to provide various security products and services that meet users' growing security needs.

REFERENCES

(1) ISO/IEC; Information technology - Security techniques - Entity authentication mechanisms-Part2: Mechanisms using symmetric encipherment algorithms, ISO/IEC9798-2
(2) SecureSocket, http://www.hitachi.co.jp/Prod/comp/soft1/secsoc/

ABOUT THE AUTHORS

Makoto Kayashima
Joined Hitachi, Ltd. in 1989, and now works at the Systems Development Laboratory, 7th Department. He is currently developing a security management system. Mr. Kayashima is a member of the Information Processing Society of Japan, IEICE, Japan Society for Software Science and Technology, and Japanese Society for Artificial Intelligence, and can be reached by e-mail at kayashi@sdl.hitachi.co.jp.

Yasuhiko Nagai
Joined Hitachi, Ltd. in 1985, and now works at the Systems Development Laboratory, 7th Department. He is currently developing security evaluation technology. Mr. Nagai is a member of the institute of Electrical Engineers of Japan, IEICE, and the Japan Society for Aeronautical and Space Sciences, and can be reached by e-mail at y-nagai@sdl.hitachi.co.jp.

Masato Terada
Joined Hitachi, Ltd. in 1986, and now works at the Systems Development Laboratory, 7th Department. He is currently developing Internet and network security technology. Mr. Terada is a member of the Information Processing Society of Japan, and can be reached by e-mail at terada@sdl.hitachi.co.jp.