Achieving Security in the NGN

Takemi Nisase†

Abstract

This article presents the basic ideas for achieving security in the Next Generation Network (NGN) and introduces core border defense technology based on the security model described in NGN international standards. These multilayer security functions should defend against diverse security risks and provide the same level of safety and security as conventional telephone services.

1. NGN security standardization trends

ITU-T (International Telecommunication Union, Telecommunication Standardization Sector) issued security requirements for Next Generation Network (NGN) Release 1 in April 2007 in the form of Recommendation Y.2701 [1]. This Recommendation describes security threats and countermeasures based on the eight security dimensions specified in Recommendation X.805 [2]. The NGN security trust model that became the basis for Y.2701 is shown in **Fig. 1**. This model is divided into three zones based on the trustworthiness of NGN constituent elements. The *untrusted zone* consists of equipment such as user terminals that cannot be directly controlled by the NGN provider. In other words, it indicates a zone containing equipment that cannot be trusted. The *trusted but vulnerable zone*, on the other hand, is controlled by the NGN provider and consists of equipment providing firewalls and other means of defense. In this zone, equipment and users can be trusted, but threats could come directly from the outside. Finally, the *trusted zone* consists of equipment controlled by the NGN provider and it corresponds to a zone in which both equipment and users (operators) can be trusted. In the NGN, network border elements (NBEs) in the trusted but vulnerable zone defend against diverse attacks from the untrusted zone (i.e., they engage in border defense), and for each zone, requirements that must be followed and measures that are advisable are specified. Requirements for NGN providers as specified in Y.2701 are listed in **Table 1**.

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan

Recommendation Y.2701 also describes specific requirements such as equipment hardening (no *backdoors*), audit trails, logging, time stamping, resource allocation and exception handling, code & system integrity and monitoring, and session initiation protocol (SIP) pinhole control.

2. Achieving security in NTT's NGN

Taking into account the services to be provided, the standardization trends described above, and Internet attack trends, NTT's aim for its NGN is to provide a *safe and secure* network infrastructure by means of a multilayer defense approach that executes security measures at each element of the NGN. In the following, I describe defense functions corresponding to NBEs, which are a distinctive feature of the NGN (**Fig. 2**).

(1) Access control for entire network

By blocking packets from/to private address spaces using an NBE-equivalent function, the NGN limits reachability from points outside the NGN (outside terminals and other networks) unnecessary for its services to points within the NGN (network equipment and various types of servers) (Fig. 2(i)). This function reduces unauthorized access across the entire network.

(2) Mitigating attacks by preventing spoofing

The NGN uses an NBE-equivalent function to prevent spoofing-related attacks that misrepresent the source IP (Internet protocol) address or originating telephone number (Fig. 2(ii)). This function mitigates various attacks made possible by misrepresenting the source IP address (e.g., session disconnect attack caused by a false message assuming the source IP

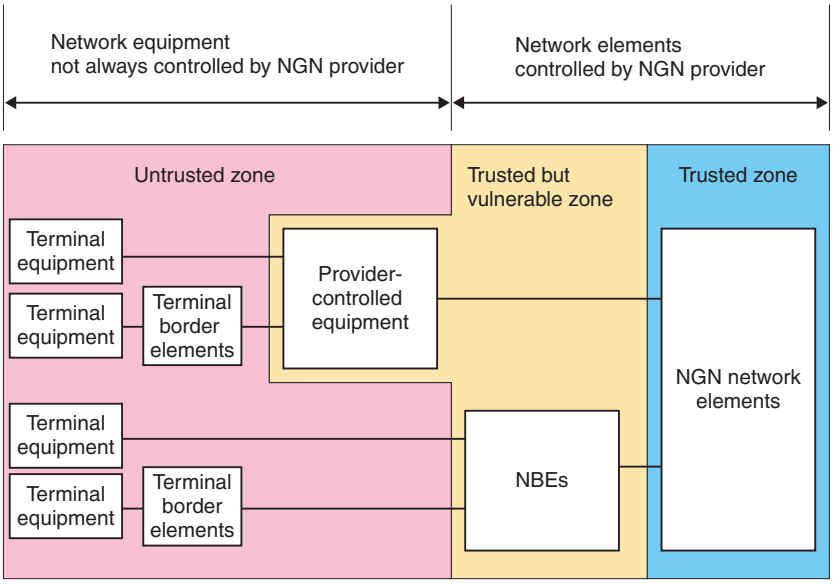

Fig. 1. NGN security trust model (ITU-T Y.2701).

Table 1. Main security requirements in Y.2701.

Eight dimensions of ITU-T X.805	Main security requirements for NGN providers in Y.2701
(1) Access control	• Restrict access to authorized subscribers.
(2) Authentication	• Able to authenticate subscribers, equipment, network elements, and other networks.
(3) Non-repudiation	• Not specified
(4) Data confidentiality	• Protect the confidentiality of subscriber traffic by cryptographic or other means. • Protect the confidentiality of control messages by cryptographic or other means. • Protect the confidentiality of management traffic by cryptographic or other means.
(5) Communication security	• Provide a mechanism for preventing the interception of information.
(6) Data integrity	• Protect the integrity of subscriber traffic by cryptographic or other means. • Protect the integrity of control messages by cryptographic or other means. • Protect the integrity of management traffic by cryptographic or other means.
(7) Availability	• Able to prevent communications with a non-compliant user terminal to mitigate DoS attacks and the spread of viruses. • Provide disaster-recovery functions and procedures.
(8) Privacy	• Protect the subscriber's private information such as location data, IDs, phone numbers, and call-accounting information.

DoS: denial of service
ID: identity

address of the attack target, denial-of-service (DoS) attack exploiting replies to the misrepresented address, and other attacks that conceal the source of the attacks). The correspondence between source IP addresses and access lines can also be managed so that a source IP address can be investigated upon the detection of attack-like packets and the originating access lines of the attacking packets can be determined.

(3) Protection of SIP-controlled communications

The NGN provides a particularly robust defense function for SIP-controlled session-based communications that have quality and reliability requirements. Specifically, the NGN uses an NBE-equivalent func-

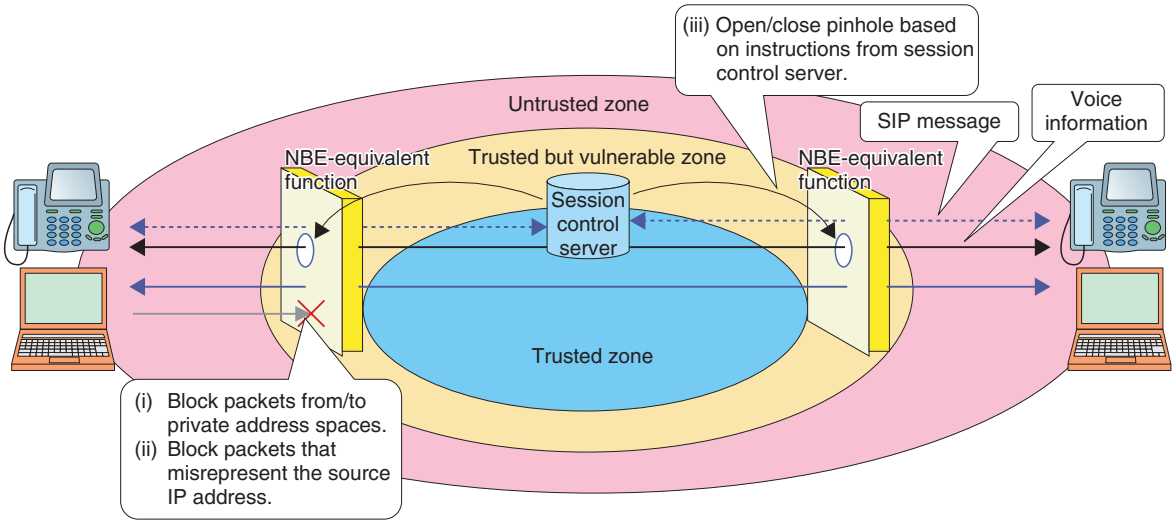

Fig. 2. Border defense by NBE-equivalent functions.

tion linked to SIP messages to open and close a *pinhole* so that communications between terminals whose session has been established by SIP messages can use a priority bandwidth (Fig. 2(iii)). By allowing only SIP-controlled communications to use a priority bandwidth, this function can prevent the harmful effects of attacks that use large volumes of traffic from other users, so it ensures stable communication performance.

3. Concluding remarks

The basic design and basic functions of the NGN aim to make it difficult for attacks to occur and to enable the source to be determined if an attack should occur. However, as NGN services progress, we can expect to see new types of attacks and risks. To deal quickly with these risks and achieve *safety and security* on an ongoing basis, we will push forward in our research in collaboration with system developers and operators. We will strive to create an even safer and more secure network by combining these basic functions with the defense functions installed in each piece of network equipment.

References

[1] ITU-T Recommendation Y.2701, "Security requirements for NGN release 1," Apr. 2007.
[2] ITU-T Recommendation X.805, "Security architecture for systems providing end-to-end communications," Oct. 2003.

Takemi Nisase
Senior Research Engineer, Secure Communication Project, NTT Information Sharing Platform Laboratories.
He received the B.E. and M.E. degrees in electronic engineering from Tohoku University, Miyagi, in 1985 and 1987, respectively. He joined NTT Laboratories in 1987. Since then, he has been engaged in research on ATM voice communication (VTOA), VoIP (Voice over IP), and secure IP communication (IP-VPN). He is currently engaged in research on Internet security technology.