Network Security R&D for Safe and Secure Communications

Ichizo Nakamura† *and Hiroki Masuda*

Abstract

NTT Information Sharing Platform Laboratories is researching and developing network security technologies and responding to security incidents to protect the network from an increasing number of security threats and provide NTT customers with safe and secure communications.

1. Introduction

NTT Group's Medium-Term Management Strategy calls for the creation of a *safe, secure, and convenient communication network environment and broadband access platform for its customers*, and the NTT Corporate Social Responsibility (CSR) Charter states that *safe and secure communication* is a pillar of CSR. In this way, NTT Group companies are working together to provide customers with even better services that they can use with full confidence in their safety. As part of this effort, NTT Laboratories is engaged in various security-related research and development (R&D) projects toward safe and secure communications. This article introduces the security environment surrounding the network and the network security R&D at NTT Information Sharing Platform Laboratories.

2. Security environment surrounding the network

In its early days, the Internet was simply an auxiliary means of communication, but now, after a period of explosive growth, it has become an indispensable part of daily life. These days, various types of security-related incidents can occur on the Internet, such as the leakage of personal and corporate information, infections by computer viruses, intrusion and tampering of computer systems by hackers, and attacks by botnets on the systems of particular enterprises. Today, with the Internet taking on the role of a social infrastructure, such security problems can have a big impact on society extending beyond the level of computer damage. For example, a computer system crash can bring the business activities of an enterprise to a halt, and the leakage of personal information can damage a company's reputation. To make matters worse, the expansion of the broadband network, dramatic jumps in computer processing ability, advanced applications, and the provision of highly convenient services have only made it easier for malicious persons to devise new attacks. As a result, security threats are increasing on a daily basis.

3. Network security R&D at NTT Laboratories

In the face of the ever-increasing security threats, NTT Information Sharing Platform Laboratories researches and develops network security with the following three objectives in mind (**Fig. 1**).

1. Protect the network itself from security threats
2. Protect systems from security threats via the network
3. Improve the security level of the entire NTT Group

As a network carrier, maintaining the infrastructure maintenance and providing stable communications are important for NTT in fulfilling the first objective. Network security R&D can be broadly divided into two approaches to security threats:

- Mitigate their impact
- Prevent their occurrence.

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

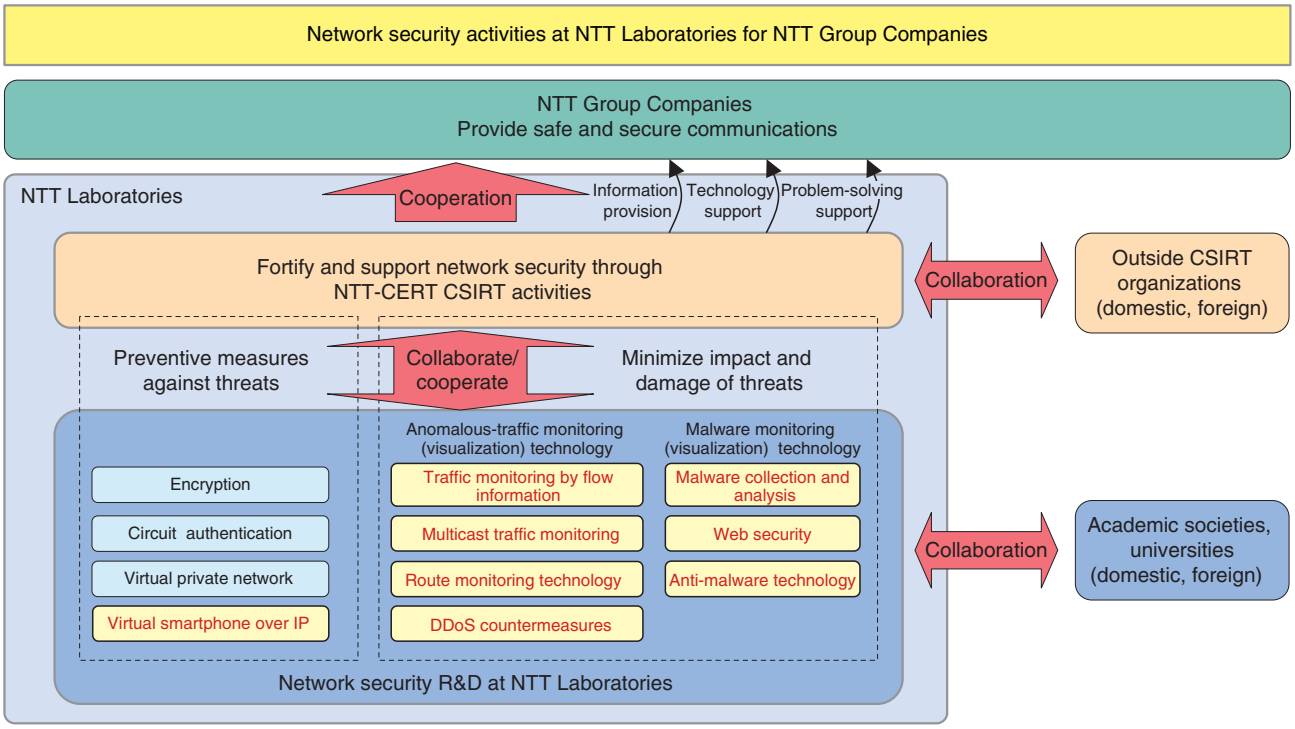

Fig. 1. Network security activities at NTT Laboratories.

Although the Internet started out as a modest framework, it has rapidly evolved into a complicated entity. As a result, it has entered a state in which new problems occur on a daily basis, which makes the impact mitigation approach the more urgent of the two.

NTT Information Sharing Platform Laboratories is focusing its attention on *traffic monitoring and analysis technologies* and *anti-malware technologies* as R&D for mitigating the impact of security threats. It is also striving to improve the security level of the entire NTT Group through its NTT-CERT incident–response team. Furthermore, to prevent the occurrence of security threats, which is the ultimate approach toward a prime solution, NTT Information Sharing Platform Laboratories is working on the development of virtualization technology for mobile phones—virtual smartphone over IP—as one idea for technology for this purpose. These topics are described in detail in the other articles in this Special Feature.

4. Traffic monitoring and analysis technologies

The Internet is becoming a new lifeline in society, and improving service continuity is becoming increasingly important. However, with the upgrading of access circuits to broadband speeds, the impact of distributed denial of service (DDoS) attacks and other types of malicious activity is now extending to the backbone network. As a result, attacks have come to embroil not only direct victims but also many indirect victims who cannot make use of the Internet owing to the damage wrought by such attacks. To solve this problem, the network must be defended in a comprehensive manner, but a huge amount of traffic flows through the backbone network, which makes detailed monitoring far from easy.

To deal with this situation, one effective technique is to sample and collect flow information from the entire backbone network and to monitor traffic fluctuations continuously using, for example, NetFlow protocol, and if an anomalous traffic fluctuation is detected, to analyze and identify the source and destination of that traffic. It is also effective to analyze in detail network control information such as domain name system (DNS) queries and border gateway pro-

tocol (BGP) routing information from the very start since even a small amount of anomalous traffic can have a big impact on the entire network.

Against the above background, NTT Information Sharing Platform Laboratories is researching and developing technologies for monitoring and analyzing traffic flowing through the backbone network by taking a multifaceted approach that combines the above techniques.

5. Anti-malware technologies

Malicious software such as computer viruses is called malware. Although Internet-based services have come to support our daily lives, significant incidents, such as the leakage of personal or corporate information via the network and the falsification of information on websites, are on the increase with many occurring through the use of malware. An attacker can infect personal computers or servers with malware and control it remotely. Malware can also be used to launch DDoS attacks and send floods of spam email—it can be thought of as the source of cyber attacks.

The methods used for infecting users' computers and servers with malware are becoming increasingly complicated and sophisticated so it is becoming very difficult to detect infections. In addition, the interaction between malware programs and the increase in malware subspecies is exacerbating the situation.

Decoy systems called *honeypots* that can be used for detecting malware infections are being researched and developed. The results obtained by using honeypots can be used to create countermeasures to malware. For example, it is possible to filter communications from users' computers and servers to destinations that causes malware infection on honeypots. For such countermeasures, it is also effective to collect and analyze malware technologies. NTT Information Sharing Platform Laboratories is researching and developing technologies for detecting malware infection activities, collecting malware, analyzing infection routes, and analyzing the malware itself.

6. NTT-CERT

In addition to basic R&D of network security, NTT Information Sharing Platform Laboratories is exploiting the technologies and know-how of NTT Laboratories to improve the security level of the entire NTT Group through NTT-CERT, a Computer Security Incident Response Team (CSIRT) organization.

CSIRT is a framework for analyzing and responding to computer incidents and educating people about them. It acts as a point of contact for security incidents that occur in NTT Group companies, helps companies to respond effectively to incidents, and disseminates security-related information.

NTT-CERT activities are supported by a diverse range of security-related know-how accumulated by NTT Laboratories with a focus on network security technologies. NTT-CERT is also constructing a cooperative framework to promote collaboration with domestic and foreign CSIRT organizations, the Nippon CSIRT Association, and outside, hub-like organizations like the Forum of Incident Response and Security Teams that brings together various CSIRT organizations. This cooperative framework is expected to promote the exchange of security-related information and incident know-how, which should be useful in responding to incidents in the NTT Group.

7. Concluding remarks

NTT Information Sharing Platform Laboratories is actively involved in R&D of network security technologies. It promotes NTT-CERT activities that make use of these technologies and contributes to the provision of safe and secure communication services in the NTT Group. Its ultimate objective through these R&D efforts is to provide NTT customers with safe and secure communications. In future research, NTT Information Sharing Platform Laboratories will turn its attention to the second of the two approaches introduced above—preventing the occurrence of security threats—in addition to mitigating their impact.

Ichizo Nakamura

Project Manager, Secure Communication Project, Information Security Project, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.E. degrees in electrical engineering from Keio University, Kanagawa, in 1984 and 1986, respectively. Since 1986, he has been working at NTT Laboratories. His current research interests include network security (technologies for protecting network services from DDoS and/or Malware attacks, and CSIRT activities (NTT-CERT) and technologies for protecting network services from DDoS and/or malware attacks). He is a member of the Institute of Electronics, Information and Communication Engineers of Japan.

Hiroki Masuda

Senior Research Engineer, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.E. degrees in physical science from Tsukuba University, Ibaraki, in 1990 and 1992, respectively. He joined NTT in 1992. He is currently engaged in developmental research on network security.