Spotlight on NTT Laboratories

Developing High-security Technology for High-reliability Networks

Atsuhiro Goto
General Manager, NTT Information Sharing Platform Laboratories

Situated inside the Musashino R&D Center, NTT Information Sharing Platform Laboratories fills a vital role in the NTT Information Sharing Laboratory Group through research and development of security technology indispensable for the network society. We sat down with General Manager Atsuhiro Goto and talked about new technologies developed at the laboratories.

Role of NTT Information Sharing Platform Laboratories

—Dr. Goto, please explain the role of NTT Information Sharing Platform Laboratories at NTT.

NTT Information Sharing Platform Laboratories lies under the umbrella of the NTT Information Sharing Laboratory Group. Our main mission is to research and develop network technology and security-related technology related to the information-sharing platform. Making use of network functions, we provide the functions and overall mechanism needed to develop safe and secure services.

There are three main types of technologies associated with the keywords *safe* and *secure*. The first is encryption technology for encrypting data and preventing information leaks. The second is network security technology for operating the network in a safe and secure manner. And the third is platform technology to provide service providers with a comprehensive set of essential functions. The role of the Information Sharing Platform Laboratories is to skillfully combine these three types of technologies to provide safe, secure, and convenient information-sharing network services.

—Could you give us an example of important technology developed at the Information Sharing Platform Laboratories?

In 2000, NTT developed a 128-bit block cipher called Camellia as a joint project with Mitsubishi Electric Corporation [1]. Camellia is Japan's representative cipher using a common key. It is capable of high-speed and highly flexible implementations in accordance with the user environment, and it can be used even for smart cards having a relatively small amount of onboard memory and for USB-based portable media (USB: universal serial bus).

This technology is provided through a royalty-free licensing system. In this way, NTT hopes to contribute to an environment in which this technology can be widely used both inside and outside Japan and to play a leading role in the creation of a low-cost, safe, and advanced information-sharing society. On the technical side, Camellia has been recognized as an international standard *having equivalent security and performance in many respects to AES (advanced encryption standard), the standard cipher of the United States government*, and it has come to be used widely in open-source operating systems like Linux and free browsers like Mozilla Firefox.

The bright side and dark side of ICT

—ICT brings much convenience into our lives, but it has harmful effects as well, doesn't it?

Yes, as a fundamental technology, information and communications technology (ICT) can make our lives very convenient, but it unfortunately has a dark side too. In recent years, there has been much abuse and many criminal acts and incidents. For example, criminal activities targeting vital government systems and malicious behavior such as impersonating (spoofing) someone else during online shopping is on the increase, and the methods used in such activities are becoming more elaborate and ingenious every year.

In the area of network security, there seems to be no end to incidents of *phishing*, in which a fake web page that looks exactly like that of a bank, for example, is created in order to trick customers and steal IDs and passwords that are needed to access customer PINs (personal identification numbers) and other personal information. In addition, viruses are coming to be embedded not only in email, but also in Web sites and freely distributed software, so it is imperative that we do not relax our guard against such threats.

—How do you cope with the dark side of ICT at the Information Sharing Platform Laboratories?

Well, to begin with, it's not simply a matter of creating anti-virus software to get rid of viruses—that's not what we do. Instead, we work to develop analytic technology to determine the risk posed by actual viruses and develop defensive technology for dealing with the myriad of attacks lurking out there on the network.

We must also collaborate with network-related parties inside and outside Japan to deal preemptively with risk that occurs when using a network. To this end, the Information Sharing Platform Laboratories is tying up with Japanese companies as well as overseas companies that collect network-related information. We are also researching the field of security management as it relates to systems and operations to determine how best to maintain network security and tackle security problems such as information leaks.

Furthermore, with the aim of building a service platform that will support the creation of many safe, pleasant, and convenient services, we are researching and developing the key elements of such a platform, including encryption algorithms, authentication schemes, and IDs, plus IPv6 (Internet protocol version 6) next-generation Internet technology.

New authentication schemes supporting the network society

—Can authentication be made simple yet robust to attack?

The authentication method commonly used today on the Internet is to enter an ID and password to log in. However, since someone's ID and password could be used by someone else, there are some situations, such as the sending of remittances, where one login is not sufficient and the user is asked to enter a different ID and password in addition to make the authentication process more secure. Against this background, Information Sharing Platform Laboratories has been researching and developing authentication schemes that can achieve higher levels of reliability and safety while being simple and hassle-free from the user's point of view.

One example is technology for identifying what circuit a customer is using when logging on to a network service from a home personal computer. In this case, the authentication process would reject the request not only if the ID and password entered by the user did not match, but also if the circuit being used was a mismatch. For example, an attempt at withdrawing another person's savings from an online bank over the Internet using a stolen ID and password would fail if the circuit being used was identified as being different from the one originally associated with that ID and password.

In this way, research is progressing on the upgrading of security by performing ID/password authentication simultaneously with circuit identification. Of course, this scheme assumes access from a home, and since scenarios in which users wish to be authenticated at locations outside the home have been increasing in recent years, we foresee the need for authentication and identification technology more suited to the mobile age.

—Isn't it possible to take the initiative and destroy new viruses and prevent network attacks before they do any damage?

It's possible, but perhaps that's not what we want to do. A system that insulates itself from all risk may be very inconvenient and not so user friendly.

To give an example, we may imagine completely

eliminating all crime and traffic accidents, but is that really possible or desirable? To eliminate all crime, there would have to be about one police officer for every two people, which would incur huge costs. And to eliminate traffic accidents, we would have to eliminate all cars, which is not very realistic.

Similarly, in the case of systems, no doubt you would agree that we have come to expect an assurance of safety with just the right balance between security and cost. Of course, even if viruses were to be scattered all over, we can consider what might happen if no one responded to such trickery: Those involved in the creation of viruses might find it less appealing and might not create them any more, so the number of viruses in the network just might decrease.

When thinking, as a human society, about the extent to which security should be implemented, the problem must be approached from many angles, from its social and psychological aspects to its relation with legal and social systems. In the end, the problem of security involves people, to be sure, but also the social system and its laws to protect personal information. I believe it's vitally important that we ensure system security while maintaining a balance between such opposing factors.

Necessity of collecting information on worldwide viruses and encryption technology

—Amidst the need to be constantly upgrading security technology, what kind of issues do you face?

Well, to give an example, encryption technology comes in various forms, and because such technology is incorporated in all kinds of systems, identifying and understanding all these different encryption techniques is not a trivial task. Another aspect of this problem is the difficulty of collecting information on how such technology affects systems and networks.

Nevertheless, in order to make improvements in security technology, we need information on where and how to make these improvements to best effect and where to incorporate new technology as well. I feel a great need for a mechanism and system that can collect and interpret such information on an ongoing basis.

—Dr. Goto, what does the future hold for the Information Sharing Platform Laboratories?

To begin with, we are now gearing up for the full-scale commercialization of the Next Generation Network. In addition to the NTT Group, a variety of service providers plan to roll out a wide array of services. Thus, the question is how these services will be supported from a security point of view. At the Information Sharing Platform Laboratories, we are working to provide safe and secure networks and services through the means of encryption and authentication.

The policies behind R&D at the Information Sharing Platform Laboratories will not change in the years to come. We will continue to make regular security upgrades to make services safer and more robust to new viruses and attacks, to research technology that can quickly and easily uncover viruses that target network vulnerabilities, and to research security technology that is easier to use and more convenient while being more robust to threats.

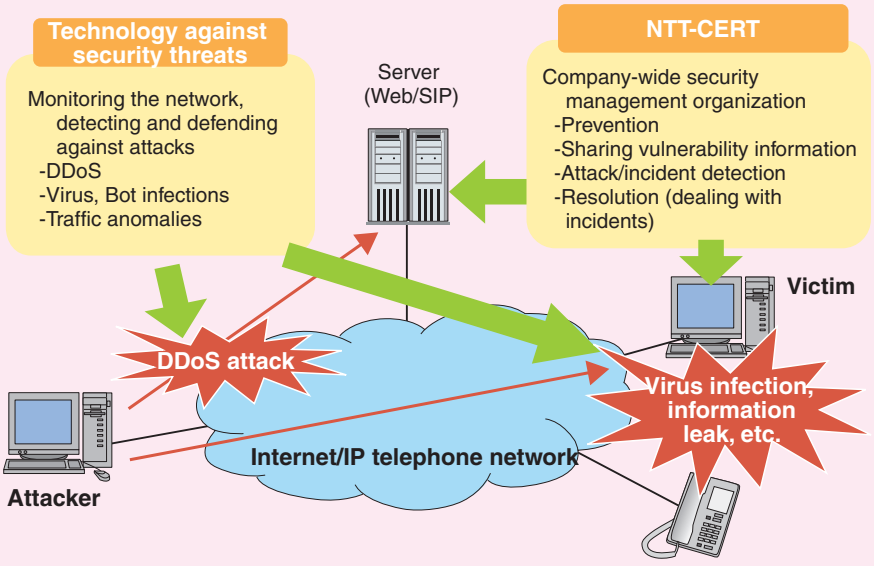
Reference

[1] M. Kanda, "Promoting the Use of Camellia," NTT Technical Review, Vol. 4, No. 2, pp. 49–53, 2006.

Notable activities at NTT Information Sharing Platform Laboratories

R&D in network security

The focus of R&D in network security, a major endeavor at NTT Information Sharing Platform Laboratories, is outlined in **Fig. 1**. This work involves contacting related laboratories in NTT about traffic anomalies, virus detection, and network faults, taking provisional and ongoing measures, and analyzing and researching viruses and network vulnerabilities, all while interacting with concerned group companies as part of a Plan-Do-Check-Act (PDCA) cycle.



NTT-CERT: NTT Computer Security Incident Response and Readiness Coordination Team
SIP: session initiation protocol
DDoS: distributed denial of services

Fig 1. R&D in network security.

R&D in information security

Figure 2 shows the R&D approach to information security taken in NTT Information Sharing Platform Laboratories, including encryption technologies and information leakage measures technologies. These technologies are essential to safe and secure use of the network. The Camellia encryption technology introduced in this article is one example. It is the first Japanese cipher to be adopted as an Internet standard cipher and as an ISO/IEC (International Organization for Standardization, International Electrotechnical Commission) international standard cipher. As explained on NTT's cipher Web site, the name Camellia refers to the flower called *tsubaki* in Japanese. Its scientific name is *camellia japonica*. Given that this encryption technology originated in Japan, it was only fitting that it be given the name of a plant that is native to Japan.

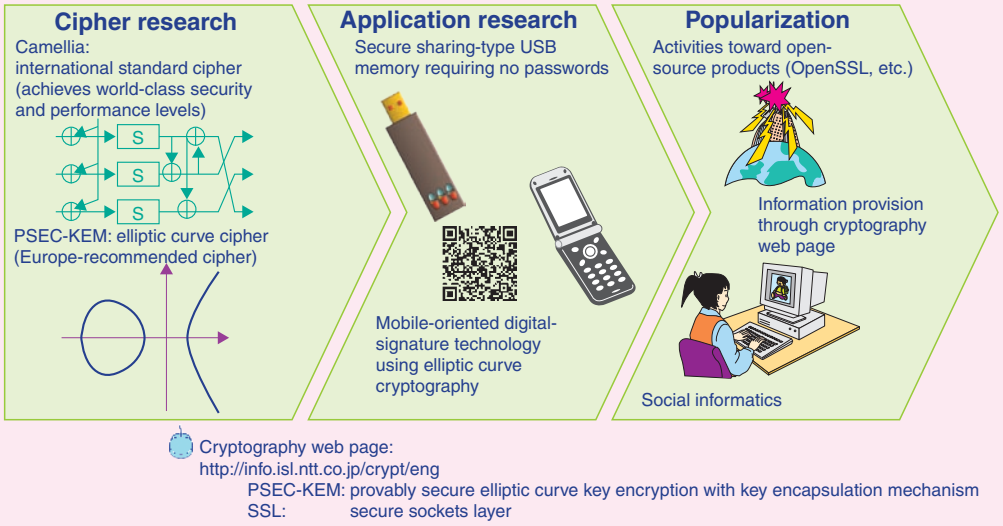


Fig 2. R&D in information security.

An expert in encryption technology at NTT Information Sharing Platform Laboratories

In April 2007, NTT officially introduced the NTT Fellow program within the NTT Group. The title of *fellow* is given only to researchers with outstanding achievements and worldwide recognition. Since the launch of this system, two researchers have been designated fellows: Dr. Takehiro Moriya of NTT Communication Science Laboratories and Dr. Tatsuaki Okamoto of NTT Information Sharing Platform Laboratories. Dr. Okamoto is a world-renowned authority on public-key cryptography. As head of the Okamoto Research Laboratory at Information Sharing Platform Laboratories, he plays a leading role at NTT.

Picking up fallen leaves in late autumn

Musashino R&D Center, home of NTT Information Sharing Platform Laboratories, is located in a quiet residential neighborhood in Tokyo's Musashino City. Last December, during the preparation of this article, a sidewalk lined with ginkgo trees leading up to the Center was awash in vivid yellow colors (**Photo 1**). Various types of trees are also planted within the premises, and at this time of year, their leaves start to fall, becoming scattered even outside the laboratory grounds. From November to mid-December, these leaves are picked up by volunteers from the Center every Wednesday during lunchtime to do their part in keeping the neighborhood beautiful.

Photo 1. Row of ginkgo trees.