R&D Spirits

Secure and Reliable Technology for Network Services

Tomoo Fukazawa
Executive Manager
Secure Communication Project
NTT Information Sharing Platform Laboratories

While the Internet has become an indispensable infrastructure of society, network security is being threatened by an ever increasing level of antisocial and criminal activities. The Secure Communication Project at NTT Information Sharing Platform Laboratories is researching and developing countermeasures from the viewpoint of a telecommunication carrier. We sat down with Tomoo Fukazawa, Executive Manager of this project, to find out what problems must be solved to provide secure and reliable network services.

Pursuing a secure communication infrastructure from three points of view

—Dr. Fukazawa, what research theme are you currently working on?

In the Secure Communication Project, the purpose of our research is to enable secure and reliable network construction and service provision across all layers. In order to provide secure communication network, it is not enough to take partial measures dealing only with the network or only with operations. Recognizing that the partial approach is inadequate, we formed a team of about 50 researchers and organized them into three main groups to address virtual private network, architecture of secure network for the Internet, and operation issues through activities such as technology development and standardization toward secure communication. My role is to manage all of these activities.

—What research in particular is each of these groups involved in?

Well, at the network level, we are researching technology for providing next-generation virtual private networks (VPNs) called Global Area Virtual Ethernet Services (GAVES) (**Fig. 1**). Furthermore, as part of a National Institute of Information and Communications Technology (NICT) project overseen by the Ministry of Internal Affairs and Communications, we are working mostly on band-width mapping and switching control in research on a next-generation terabit-class supernetworking architecture. Next, at the secure network for the Internet level, we are developing technology to counteract distributed denial of service (DDoS) attacks. We called this technology “MovingFirewall” [1] (**Fig. 2**) as it aims to activate firewall functions across the entire network. Finally, at the operations level, we have organized a computer security incident response team (CSIRT) called NTT-CERT (**Fig. 3**) that responds to security incidents, collects and disseminates security-related information, and performs various educational services in addition to linking up with other CSIRT teams throughout the world.

—What are some of the technical features of this research?

Speaking of GAVES, we are promoting an extension of wide-area Ethernet services that excels in scalability, maintainability, and operability. In this regard, a network may be an “L2” (layer 2) type referring to the Ethernet network or an “L3” type referring to an IP (Internet protocol) network. The GAVES scheme targets an L2 network. While an L2 network possess-

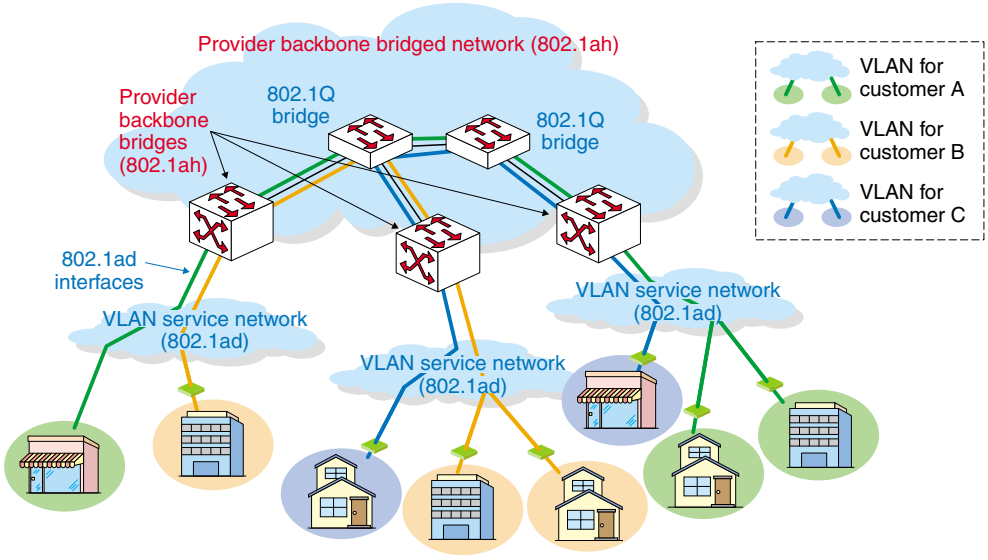

Fig. 1. GAVES: 802.1ah provider backbone bridges.

es generality, it has poor scalability, and it is not an end-to-end protocol, so network faults are difficult to handle. In contrast, the GAVES scheme that we favor can solve all of these problems in L2-network operation. This protocol is also compatible with the IEEE P802.1Q and IEEE P802.1ad L2 standards and allows existing services to function without modification.

We found that MovingFirewall is an effective countermeasure against DDoS attacks, which have become a significant threat to the Internet in recent years. A DDoS attack is a sort of "time bomb" directed at a particular server. A virus planted on a computer by someone with malicious intentions spreads out over the network and infects many servers prior to the time of the attack. At a predefined moment, a huge number of packets destined for the targeted server are released in unison throughout the world thereby tying up the services provided by that server. Starting in about 2000, a number of well-known servers used for e-commerce and computers systems became the target of DDoS attacks. A single server or computer, however, is unable to deal with an attack mechanism of this type. Moreover, current countermeasures are basically manual in nature, which means that they take time to implement. Therefore, a large amount of damage can occur before the attack is repulsed. We developed MovingFirewall to automate the DDoS-attack response. MovingFirewall is a system that protects the network and user servers from a DDoS attack by positioning itself at provider and data-center edge nodes in an autonomous-distributed manner. When MovingFirewall equipment senses an attack (**Fig. 2**(1)), it notifies upstream MovingFirewall equipment of the attack so that measures to control abnormal traffic can be started and information about the attack can be conveyed further upstream (Fig. 2(2)). In this way, the source of the attack can be isolated and malicious packets can be cut off at the source (Fig. 2(3)). This system ensures secure and reliable business operations even on the basically open Internet used by an extremely large number of diverse users. We are already conducting field trials with demo equipment, and since we are obtaining fairly good results, I believe we can market MovingFirewall fairly soon.

In addition to the above system-development work, NTT-CERT is constructing platform technology from the viewpoint of security-related operations. Specifically, this team is working to produce operation methods for maintaining security, provide training for security technicians, evaluate commercial security products, and collect and distribute security information. This buildup of operations-related know-how is of vital importance for actual on-site maintenance of security.

—What problems do you face?

One is cost. If we were to pursue a secure and reliable network without limits, then the cost would know no bounds either. However, that is not a realistic approach. One problem that must be addressed when implementing security technology is how to efficiently construct an effective system while taking cost into account. Another problem is speed. Unfortunately, network-threatening attacks are increasing every year, and it is vital that we create a viable

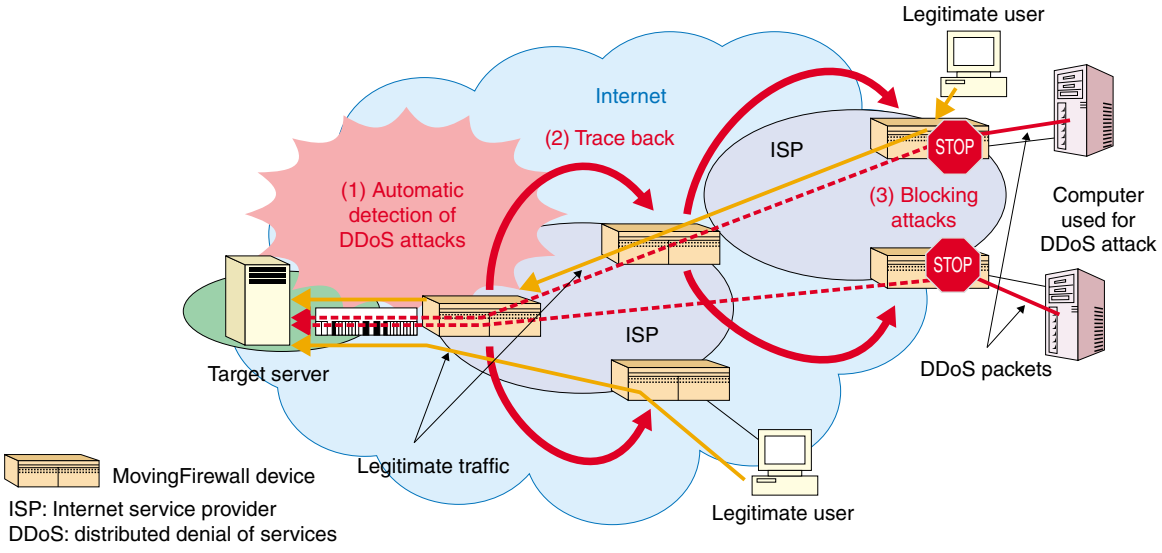

Fig. 2. MovingFirewall: network device for defending against DDoS attacks.

response system as soon as possible.

More specific problems include phishing and spam mail. Phishing is an act of fraud—it attempts to acquire personal information by impersonating an actual e-commerce site. Spam mail, on the other hand, is annoying unwanted mail that usually arrives in large volumes much to the exasperation of the receiver. But only by the simple traffic observation from the outside in the network layer, it is difficult to judge either phishing or spam mail to be abnormal. In contrast to viruses, these are threats that are difficult to detect automatically on the system side. To combat these problems, a more precise security mechanism must be created through traffic analysis and control or analysis that takes upper-layer protocol into account. Another major problem is the development of security measures for future IP networks geared to telephone services.

—How do you think this research will develop in the years to come?

Existing security measures are basically reactive—they respond after the fact or defend against known threats. But ideally, a defense should be mounted before damage occurs and should also counter unknown threats and attacks. For this reason, the next step in security research is to determine how to sense the signs of improper information distribution such as viruses and spam mail and how to deal with them. Since NTT is a carrier, the field of traffic analysis and control is one of our specialties. I myself, have a deep interest in this field, and naturally would like to research and develop solutions in this area making full use of the advantages that we have as a carrier. I would also like to make proposals on how networks should be constructed from the viewpoint of security.

The birth of standardization activities through linkups with other companies

—Dr. Fukazawa, what are some current R&D trends in security technology?

Individual security technologies such as anti-virus software are being increasingly developed by software developers and other enterprises. And in terms of anti-DDoS systems like MovingFirewall, dedicated equipment for individual users and closed equipment for single providers is being developed in the United States. Other anti-DDoS technology, however, does not include network tracing techniques, so it cannot protect the network and servers from an attack in an efficient and speedy manner. At the research level, we are confident that our network-tracing system is superior, but I must admit that, at the business level, American venture companies are strong, and I think we are just about to face serious competition.

—How does security research at NTT stand out?

I think that no research elsewhere, except for carriers, considers all aspects from the network layer to operations. Considering that the Internet has become a social infrastructure, security must be treated as indispensable. Of course, individual security mea-

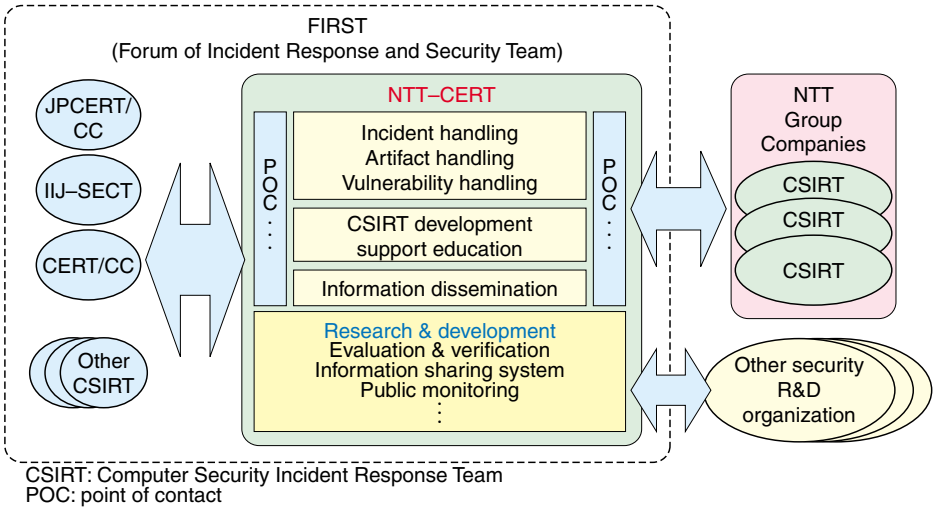

Fig. 3. Activity of NTT-CERT.

sures are also necessary, but from here on, failure to adopt a more comprehensive approach will make it all the more difficult to ensure network security. As a carrier, NTT is obligated to ensure secure and reliable communications by combining network, platform, and operation technologies. This and NTT's ability to demonstrate the effectiveness of its security measures are special features of our research.

—Are you collaborating with any other companies or research institutions?

Since NTT network has a variety of connectivities to global network, we intend to form alliances as the need arises. For example, since the effectiveness of MovingFirewall against DDoS attacks increases as more MovingFirewall equipment is installed in the network, we are considering opening up this system and spreading it to router manufacturers and Internet service providers. NTT-CERT is also moving toward international tie-ups and became a member of the Forum of Incident Response and Security Teams (FIRST), the most major international forum of expert teams, in January of this year.

—Are you involved with any other international activities such as for standardization?

Yes. We are promoting the standardization of GAVES. Standardization work on the GAVES system in the IEEE802.1 Working Group formally began in January 2005 to develop P802.1ah Provider Backbone Bridges technology for carrier-class network services.

A research career viewing "communication" from many different angles

—What made you decide to pursue computer and network research?

Well, in the first place, I found the computer to be a good tool for achieving something that had not been done before, and I also remember the interest I felt in the systematic aspects of computing. For example, some processes that take a long time and a lot of effort to perform in practice can be simulated on a computer relatively easily and immediately. And if we connect computers in a network, we can accomplish even greater things. At university, this interest led me to research high-speed parallel computing based on autonomous distributed control and network-oriented service base system based on inter-computer cooperation.

—Please tell us something about your research history?

At NTT, I was originally assigned to NTT LSI Laboratories where I researched massively parallel machines for scientific computing. At that time, I was involved with all aspects of design and development from processor development to system design and OS/application development. I even developed a simulator for designing new high-speed devices.

After that work, I continued to research computers of this type for a while, but during this research, I ran up against a big wall in relation to system testing. My research approach here was to design a system based on my ideas and then construct prototype hardware

and software. At that time, however, things didn't always work out as designed. Of course, trial and error is an integral part of the research process, and discovering that something doesn't work is not bad in itself. But as a system becomes increasingly complex, it can be extremely difficult to find out what part of the system is not working. Separating design-level and implementation-level factors is very time consuming, which can cause the development period to last longer than planned. It is also inherently difficult to verify and secure correct operation in a new and advanced prototype device. This situation caused me much distress, but during that time, I was fortunately sent to Stanford University where I studied an assertion-based system-test technique (where an "assertion" represents desired behavior) for massively parallel machines under the supervision of a hardware-testing specialist, Professor McCluskey. That was in 1989 and 1990. After returning to NTT LSI Laboratories in 1991, I incorporated hardware test techniques based on my Stanford studies into my own research and applied them to LSIs such as MPEG chips and field programmable gate arrays.

However, as processor and test technology matured, and as a debate began as to how far NTT as a carrier should pursue hardware technology, I found myself being transferred to the NTT Optical Network system Laboratories in 1995. Here, I was able to contribute to NTT's primary business and work on network technology that I had also researched at university. At these laboratories, I researched, in particular, next-generation network architecture, high-speed routers, and realtime packet filters. Then, in 1998, I was loaned out to NTT Phoenix Communications Network, Inc. (now NTT Bizlink), an NTT group company. I returned to NTT Laboratories once again in July 2004 and have since been engaged in my present research at NTT Information Sharing Platform Laboratories.

—What kind of work did you do at NTT Phoenix Communications Network?

I developed and implemented services for multipoint videoconferencing systems. I'd like to point out here that network architecture research is usually centered on IP networks, and while IP networks have very high generality, the required quality of service (QoS) depends on the application. In particular, a few packet loss or delay could be acceptable in some cases but the loss of even one packet is unacceptable in others. For this reason, I researched means of achieving an "adaptive network" that could provide various QoS levels depending on the application or service. For example, while IP excels at storing and forwarding a large amount of mail, it is weak at handling realtime communications as in telephone services. This problem is further compounded when adding images as in videophones. At NTT Phoenix, constructing an IP network for such realtime bidirectional communications was a problem in itself. But in addition, we had absolutely no idea what level of quality provided by the network would be satisfactory to customers in terms of actual services. While trying hard to figure out what level of network quality to target, I had the fortunate opportunity of learning about actual services and customer needs at a site providing videoconferencing services. As chief technical officer, I was instrumental in launching an ISDN-based videoconferencing service, in constructing for videoconferencing a high-quality IP network originally devised at NTT Laboratories, and in developing services that could interconnect IP, ISDN, and voice telephones (ISDN: integrated services digital network).

—What has been your goal in these various types of research?

My goal has been "communication", that is to connect various types of things. In videoconferencing, for example, IP, ISDN, and voice telephones—whatever customers want to use—are all interconnected. To achieve this sort of communication, I came to view the network from various angles including software, hardware, and service. And for a network in which various things can communicate freely, I noticed that security and reliability are of prime concern, which is why I am now involved with research and development related to security issues. This multifaceted approach via software, hardware, and the network is enabling me to view the research of diverse security issues in a comprehensive manner. In my research career, some things turned out as I had intended and some things did not, but all in all, I believe my career has developed quite reasonably for the research of secure and reliable communication.

NTT: Where actual services produce a treasure house of research themes

—Dr. Fukazawa, what are your aspirations for the future?

Well, as I've only begun my security research, I intend to keep with it for the time being. I am also

interested in researching services that integrate my past research on "communication" with my current research on "security and reliability." And instead of some magnificent system constructed under a long-term plan, I would rather work on creating adaptive-type systems or services that will be provided in accordance with customer or community needs.

And if I may add one more thing from a totally different perspective, I would like to disseminate the results of our research not only to the framework of NTT and Japan, but also to a world-wide audience. I would like to produce as many Japan-originating global standards as possible, and succeeding in establishing even a few would be great.

—What do you find interesting and worthwhile in R&D work?

Making possible something that has never existed or been achieved before on my own strength or the strength of our team. This is not simply because of the satisfying feeling of achievement that we feel upon solving a difficult problem, but also because of the contribution we can make to society. I feel that R&D work becomes most worthwhile when self realization and social contribution coincide.

—What is your ultimate goal as a researcher and developer?

I would like to be an engineer who has his own views within his own specialized field, whatever the goal may be. And from a position within management, where I am becoming more involved with work that is not pure R&D, I would still like to be able to view things from an engineer's perspective and give my technical opinions.

—In your mind, what kind of working environment does NTT Laboratories offer?

It is an excellent place for self realization. Research for my own purposes is connected to the further development of NTT and society, and at the same time, research for NTT and society is connected to my individual growth. This structure is well developed and functioning well. In addition, many of my colleagues and superiors are great problem-solvers and talking with them keeps me brushing up myself. I think NTT Laboratories provides a very favorable environment for researchers.

But the most wonderful thing about NTT Laboratories is its treasure house of research themes. Because of its connections to business companies, NTT Laboratories can always receive a variety of themes from sites that provide actual services. These are sometimes themes that even researchers would not have thought of. For example, while systems for handling e-mail and web communication were originally developed more than 10 years ago, developers might have imagined the possibility of phishing and spam mail, but no serious attention was paid to these problems at that time. As mail and web technologies become widely used, these problems also become serious today. Not only these problems, we have also found a lot of advanced themes to provide secure and reliable communication service as the Internet becomes widely used as the social infrastrucure. You might say that connecting with the real service fields provides not so much a treasure house but rather a wellspring of research themes. In the sense of providing unexpected, newly advanced themes to work on, I would say that NTT Laboratories is both a favorable environment for researchers and a thrilling place to work.

Reference

[1] "Development of MovingFirewall, a System that Mitigates DDoS Attacks at Upstream Nodes and Defends the Entire Network—Protecting Legitimate Traffic by Segregating Attack Traffic," NTT Technical Review, Vol. 1, No. 1, pp. 99–100, 2003.

Interviewee profile

■ Career highlights

Tomoo Fukazawa received the B.E., M.E., and D.E. degrees in electrical engineering from the University of Tokyo, Tokyo in 1980, 1982, and 1985, respectively. In 1985, he joined the Electrical Communication Laboratories, NTT, Atsugi. He became a Senior Research Engineer in 1989 at NTT LSI Laboratories. From 1989 to 1990, he was a Visiting Scholar at Stanford University, USA. In 1995, he became a Senior Research Engineer, Supervisor at NTT LSI Laboratories. He moved to NTT Optical Network System Laboratories as a Senior Research Engineer, Supervisor, in 1997. In 1998, he moved to NTT Phoenix Communications Network, Inc. as the Director of Service and Network Operations. He became Executive Vice President of NTT Phoenix Communications Network, Inc. (now NTT BizLink), in 1999. In 2003, he became Chief Technical Officer of NTT BiZLink. In 2004 he moved to NTT Information Sharing Platform Laboratories as the Executive Manager of Secure Communication Project.