Research and Development of Security Concerns Relating to Growing Threats and Business Opportunities

Kazuhiko Okubo

Abstract

The Internet of Things era has resulted in many devices with security vulnerabilities being connected to networks, and this is resulting in a rapid increase in the number of security threats in new areas such as infrastructure facilities that have up to this point been regarded as safe. On the other hand, it is also creating new business opportunities with the utilization of diverse information. This article introduces the security research and development strategy of NTT laboratories from two perspectives: defeating new threats based on an understanding of environmental changes of this nature, and strengthening the competitiveness of our business.

Keywords: security, cyber-attack, R&D policy

1. Introduction

The Internet of Things (IoT) era is close at hand. It is said that by 2020 there will be 53 billion devices of many different types connected to the Internet. In some respects, this era has already arrived. For example, we are starting to see new businesses that store diverse types of information and share it between IoT systems and cloud services to deliver improved factory productivity, self-driving vehicles, personalized recommendation services, and smart cities that are more efficient and consume less electrical power.

IoT systems and cloud services accumulate vast amounts of diverse information, and it is expected that the ability to make effective use of this information will give rise to new business opportunities. Here, an important key to the expansion of business is the development of security technology that enables the safe use of information including sensitive data such as personal data and trade secrets.

However, the IoT era also brings various security challenges. The limited processing performance and lower manufacturing costs of IoT devices make it impossible for them to incorporate the conventional security measures used in personal computers (PCs) and the like, with the result that large numbers of IoT devices with poor security are being connected to the Internet. It is feared that IoT devices of this sort could easily be hijacked and controlled via botnets, enabling them to be applied in large-scale sophisticated cyber-attacks such as distributed denial of service (DDoS) attacks. For example, a widespread power outage in one place could conceivably be caused by a cyber-attack from hijacked IoT devices. Cases in which surveillance cameras and network television services were attacked in this way have been reported. In October 2016, a large number of websites (mostly in the US) went offline, and this was also attributed to a DDoS attack from malware called "Mirai" that had been used to hijack IoT devices [1].

To prevent this sort of cyber-attack, it is essential to implement measures such as disconnecting only abnormal devices from the network while maintaining the connections of normal IoT devices when IoT

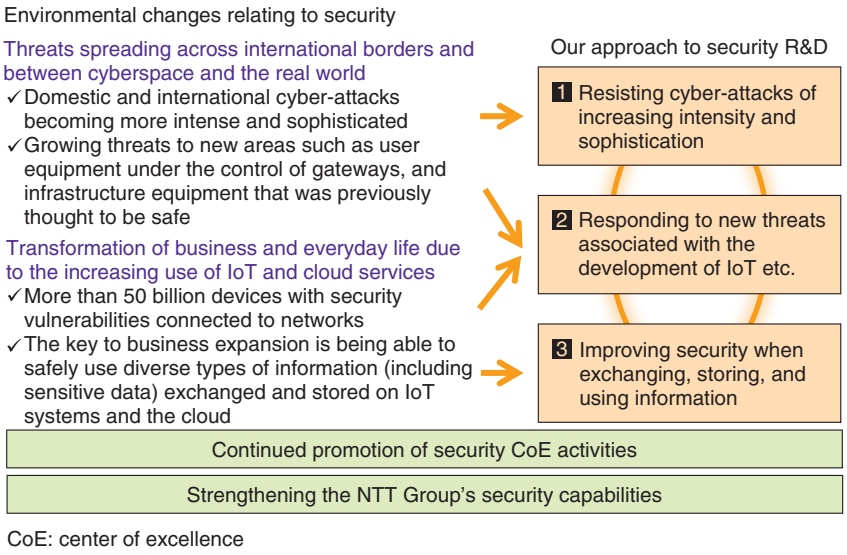

Fig. 1. Environmental changes and our approach to security R&D.

devices perform abnormal actions such as being turned into botnets.

2. Research and development (R&D) at NTT Secure Platform Laboratories

NTT Secure Platform Laboratories (hereinafter SC Labs) is conducting R&D aimed at enhancing the safety and security of cloud services and communication services provided by the NTT Group. Our mission is to create the world's most advanced security technology and to use secure technology to provide overall security improvements. To this end, our R&D is targeted at three main areas to adapt to recent changes in the security environment, as shown in **Fig. 1**. On the basis of this approach, we are carrying out a wide range of R&D from theory to the offering of product/technical know-how and operational support, with world-leading encryption technology and cyber-attack protection technology as our core competencies (**Fig. 2**).

Of the three security R&D approaches, the first two (resisting cyber-attacks of increasing intensity and sophistication, and responding to new threats associated with the development of IoT etc.) are referred to as *defense technologies* for countering cyber-attack threats, whereby we aim to contribute to improving the defenses of the NTT Group's network infrastructure and other key infrastructures. For the third approach (improving security when exchanging, storing, and using information), we are studying *offense technology* that increases the added value of NTT's products and materials used for corporate business such as cloud/network services that use IoT and services that use personal data.

2.1 Resisting cyber-attacks of increasing intensity and sophistication

At SC Labs, we are conducting R&D aimed at the creation of competitive proprietary technology and security intelligence in order to resist the growing severity and sophistication of domestic and international cyber-attacks. This is being done using our core competencies in areas such as world-leading cyber-attack detection, collection, and analysis technology while closely collaborating with group companies.

In the R&D of technology for collecting and blacklisting malicious website URLs (uniform resource locators) that cause malware infection and Internet protocol (IP) addresses that are used in attacks, we are working on information-gathering technology that emulates various web browser environments to counter malicious sites that change their behavior according to the client's web browsing environment, and information-gathering technology that deals with attacks on web application vulnerabilities, and we are operating honeypots that incorporate these results. Furthermore, we are working towards higher accuracy and broader coverage of security intelligence

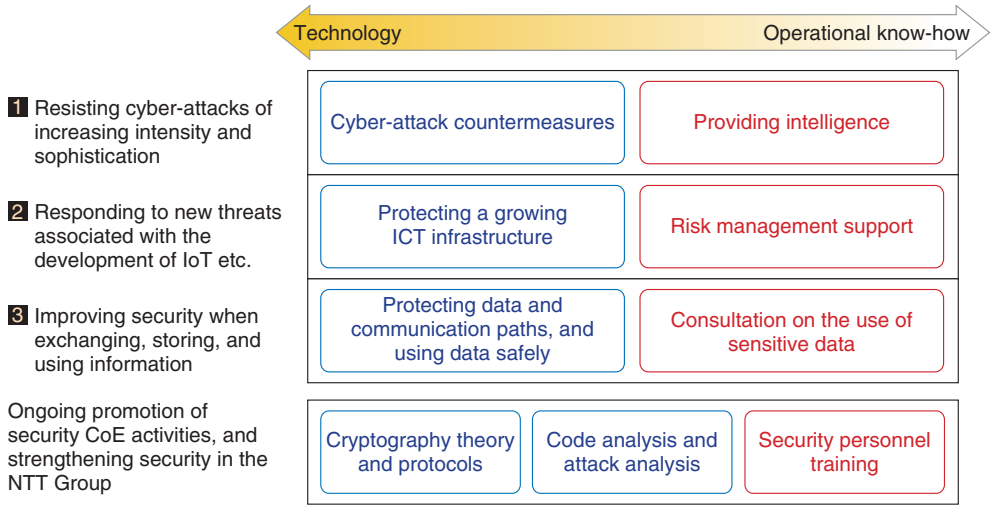

Fig. 2. Security R&D efforts.

based on advanced anti-malware technology. These technologies include dynamic malware analysis technology that analyzes the behavior of malware captured by honeypots and analyzes it by connecting to the Internet, technology for purposes such as detecting malicious HTTP (Hypertext Transfer Protocol) communication from user traffic, and technology for evaluating malicious domain names and IP addresses.

Also, in the R&D of security log analysis technology, to resist cyber-attacks that are becoming more sophisticated and harder to defend against every year, we are working on technologies including communication log correlation analysis and unknown malware detection technology that automatically extracts accurate analysis rules, and parameter profiling technology that can detect zero-day attacks with high precision.

These technologies contribute to the construction of a SIEM (security information and event management) platform aimed at strengthening the security operations of the entire NTT Group, and the development of a corporate MSS (managed security service) offered by the NTT Group.

In addition to these R&D efforts, we are also running NTT-CERT, which is a CSIRT (computer security incident response team) representing the entire NTT Group. Specifically, we are handling various types of incidents that have occurred in the NTT Group, conducting forensic studies to clarify the causes and analyze the effects of each incident, and coordinating inter-group cooperation to strengthen the group's ability to respond to cyber-attacks [2, 3].

2.2 Responding to new threats associated with the development of IoT etc.

In preparation for incidents such as the exploitation of device vulnerabilities by bots in a network environment assumed to comprise large numbers of diverse devices connected to a network, we are conducting R&D with the mission of establishing security technology related to the design, construction, and operation of secure systems that perform thorough risk assessment/management of resources that need to be protected at all stages of the life cycle.

Specifically, to improve cyber-attack defensive capabilities through integrated management of the control of systems and network equipment from a security point of view, we are working on: (1) the promotion of risk management and security through design at the system planning and design stages in order to reduce the number of incidents occurring after the system has been installed, (2) authenticity/integrity verification technology using encryption and security chips throughout the entire life cycle of connected equipment, (3) network soundness verification technology that monitors traffic and equipment status/operations of the entire network to eliminate or minimize damage, even in environments where new and old equipment are mixed together, (4) dishonest behavior detection technology that uses sensor information from a variety of IoT devices, and (5) security orchestration technology that implements

maintenance and prompt recovery of the necessary security level by performing appropriate control measures such as automatically detecting various attacks on the network.

Because devices that are connected to diverse networks in the IoT era will also be subject to diverse security threats in the same way as PCs and smartphones, it is also necessary to consider countermeasures. Although self-driving vehicle technology is in the spotlight as a symbol of the IoT era, its success depends on the implementation of cybersecurity measures in advanced vehicle control systems. In practice, cyber-attacks against vehicles, such as forcing them to operate incorrectly via a network, are starting to become a problem, and at SC Labs, we are considering applicable threats and countermeasures when vehicles are connected to networks.

These initiatives are introduced in detail in the articles "Secure Architecture for Critical Infrastructure" [4] and "Cyber-attack Countermeasures for Cars" [5] in the Feature Articles in this issue.

2.3 Improving security when exchanging, storing, and using information

To implement a safe and secure information distribution infrastructure, we are working on techniques for the secure use and operation of ciphers and techniques for the formation of encryption systems in order to keep data safe based on world-leading encryption technology and the cryptographic research on which it is based.

Interest in the use of personal data and trade secrets has grown rapidly following revisions to the Act on the Protection of Personal Information in September 2015 in Japan. However, due to difficulties in the case-by-case application of statutory requirements and the derivation of legal and useful data processing methods, advances in the utilization of sensitive data have not met expectations. At SC Labs, we are contributing to improving the added value in operating companies' security products by providing safe data utilization technology such as anonymization methods and secret computation methods, and consultation relating to the use of sensitive data in different applications and legal risk assessments of security and privacy issues.

Also, confidence in the reliability of service providers, certification authorities, and the like has been shaken due to occurrences such as frequent information leaks from businesses and interventions by state powers, and it is becoming apparent that there is a need for data protection and communication path protection measures that are less reliant on the security of servers or the morals of those that operate them. For such issues, we are working to develop technologies such as secure business chat applications that can maintain the security of communications even when information is leaked from the server, and authentication methods that can maintain security without the need for password management on the server [6].

Details of these efforts are introduced in the articles "A Secure Business Chat System that Prevents Leakage and Eavesdropping from the Server by Advanced Encryption Technology" [7] and "Key Points of the Amendments to the Act on the Protection of Personal Information, and Anonymization Methods for the Use of Personal Data" [8].

3. Future prospects

At SC Labs, with world-leading encryption technology and cyber-attack protection technology as our core competencies, we are conducting R&D that covers a wide range, from devising theories to offering product/technical know-how and operational support in order to contribute to the safety and security of cloud and communication services provided by the NTT Group.

References

[1] WIRED News on October 21, 2016. https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

[2] T. Hariu, K. Yokoyama, M. Hatada, T. Yada, T. Yagi, M. Akiyama, T. Ikuse, Y. Takata, D. Chiba, and Y. Tanaka, "Security Intelligence for Malware Countermeasures to Support NTT Group's Security Business," NTT Technical Review, Vol. 13, No. 12, 2015. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201512fa3.html

[3] F. Tanemo, I. Hayashi, M. Tanikawa, and T. Abe, "Tighter Security Operations to Help Provide Brands that are Safer and More Secure," NTT Technical Review, Vol. 10, No. 10, 2012. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa4.html

[4] M. Ueno, S. Kashima, Y. Igarashi, and M. Hori, "Secure Architecture for Critical Infrastructure," NTT Technical Review, Vol. 15, No. 5, 2017. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201705fa2.html

[5] M. Tanaka, J. Takahashi, and Y. Oshima, "Cyber-attack Countermeasures for Cars," NTT Technical Review, Vol. 15, No. 5, 2017. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201705fa3.html

[6] M. Matsui, H. Ohtsuka, T. Kobayashi, H. Okuyama, A. Nagai, and G. Yamamoto, "Milagro Multi-Factor Authentication," NTT Technical Review, Vol. 14, No. 12, 2016. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201612ra1.html

[7] R. Yoshida, Y. Okano, H. Okuyama, and T. Kobayashi, "A Secure Business Chat System that Prevents Leakage and Eavesdropping from

the Server by Advanced Encryption Technology," NTT Technical Review, Vol. 15, No. 5, 2017.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201705fa4.html
[8] K. Kameishi, K. Hirota, A. Fujimura, F. Magata, and Y. Ota, "Key Points of the Amendments to the Act on the Protection of Personal Information, and Anonymization Methods for the Use of Personal Data," NTT Technical Review, Vol. 15, No. 5, 2017.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201705fa5.html

Kazuhiko Okubo
Vice President and Head of NTT Secure Platform Laboratories.
He received a Master of Science in Management of Technology from the MIT Sloan School of Management, USA, in 2000. He joined NTT in 1989. He works at NTT Secure Platform Laboratories, where he divides his efforts between protecting the online activity of customers with security technology that can withstand even state-of-the-art cyber-attacks, and conducting research and development of technology that can strengthen our competitive edge by ensuring information can be used securely in businesses facing new threats.