Research and Development of Advanced Security Measures to Protect Customers from Sophisticated and Large-scale Cyberattacks

Kazuhiko Okubo

Abstract

The Feature Articles in this issue introduce recent trends and case studies of ever-escalating cyberattacks that are becoming increasingly sophisticated and large in scale, plus issues and needs in the security business of NTT Group companies. Additionally, new needs are arising for security measures for customers. These articles introduce the research and development of advanced technologies deemed necessary for countering cyberattacks and increasing business competitiveness.

Keywords: security, cyberattack, MSS

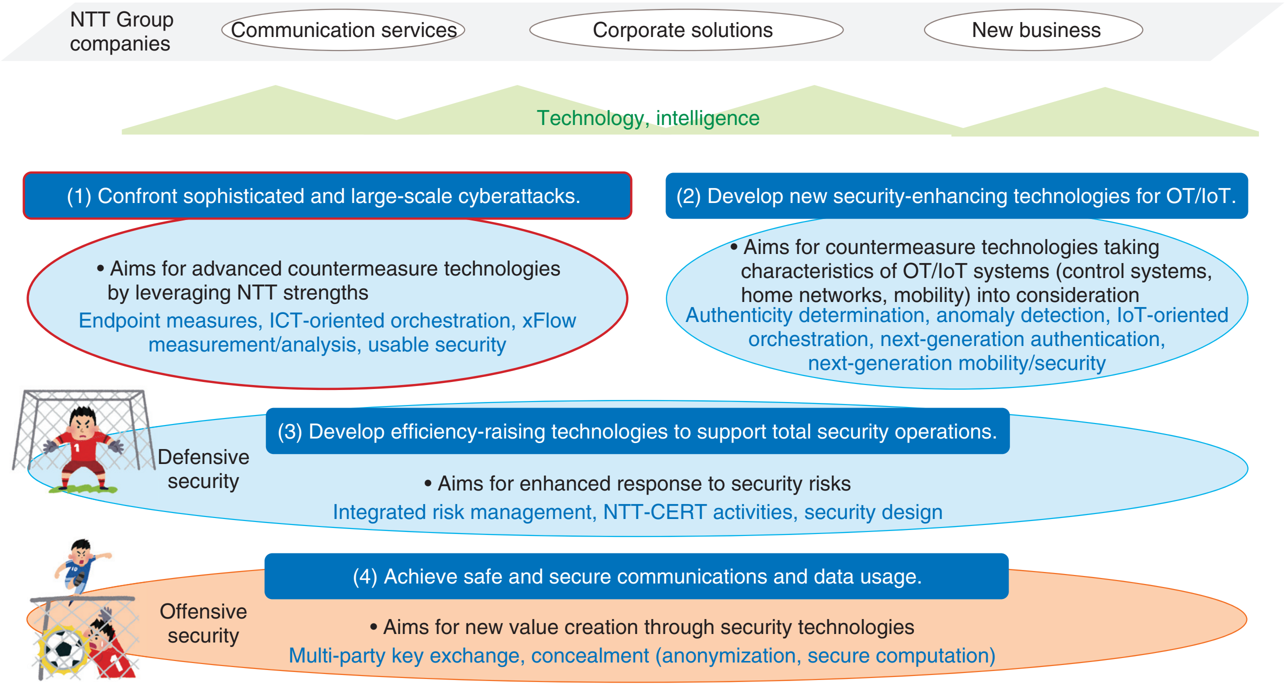
1. Changing environment in cyberspace and need for new security measures

Security threats continue to escalate due to a variety of factors. For example, cyberattack techniques are becoming increasingly sophisticated as reflected by malware with enhanced capabilities for autonomous operation. In addition, as Internet of Things (IoT) devices come to be connected in large numbers to the network despite their inherent vulnerability to security threats, large-scale distributed denial-of-service (DDoS) attacks are being carried out, with those devices used as stepping stones in their operation. Against this background, the need naturally arises for more advanced cyberattack countermeasure technologies, but there is also a need for technologies that can combat new types of security threats given the paradigm shift in the information and communication technology (ICT) environment accompanying the evolution of economic activity.

Furthermore, with Tokyo's major international sports event only about two years away, there are grave concerns about an increase in security threats against critical infrastructures and having insufficient measures to prevent and respond to incidents. Consequently, the development of technologies for securing critical infrastructures, the enhancement of comprehensive security risk management, and the development of more efficient security operations through the introduction of artificial intelligence are becoming urgent issues.

Moreover, in addition to the above *defensive* security, there is a growing need for so-called *offensive* security. This refers to the safe and secure use of data in business activities in the IoT era against the backdrop of the Japanese amended Act on the Protection of Personal Information enacted in May 2017. As a result, initiatives for avoiding risk using information security technologies including encryption and for creating new value toward economic revitalization hold great promise.

Against the background of such changes in the cyber environment and current market needs, NTT Secure Platform Laboratories has established four


NTT Group companies
Communication services
Corporate solutions
New business
Technology, intelligence
(1) Confront sophisticated and large-scale cyberattacks.
• Aims for advanced countermeasure technologies by leveraging NTT strengths
Endpoint measures, ICT-oriented orchestration, xFlow measurement/analysis, usable security
(2) Develop new security-enhancing technologies for OT/IoT.
• Aims for countermeasure technologies taking characteristics of OT/IoT systems (control systems, home networks, mobility) into consideration
Authenticity determination, anomaly detection, IoT-oriented orchestration, next-generation authentication, next-generation mobility/security
Defensive security
(3) Develop efficiency-raising technologies to support total security operations.
• Aims for enhanced response to security risks
Integrated risk management, NTT-CERT activities, security design
Offensive security
(4) Achieve safe and secure communications and data usage.
• Aims for new value creation through security technologies
Multi-party key exchange, concealment (anonymization, secure computation)

NTT-CERT: NTT Computer Security Incident Response and Readiness Coordination Team
OT: operational technology

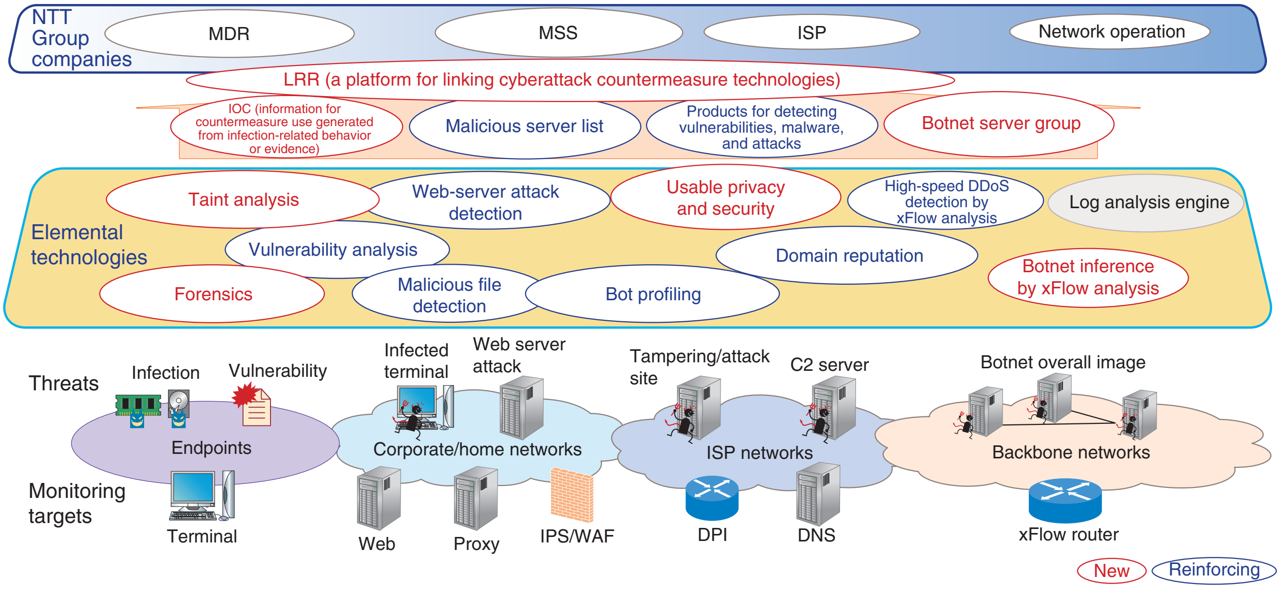
Fig. 1. Total view of security R&D.

objectives representing the pillars of its research and development (R&D) activities (**Fig. 1**). These are: (1) confront sophisticated and large-scale cyberattacks, (2) develop new security-enhancing technologies for operational technology (OT)/IoT, (3) develop efficiency-raising technologies to support total security operations, and (4) achieve safe and secure communications and data usage. Recent progress in pillars (2)–(4) was described in a previous publication [1]. Therefore, the Feature Articles in this issue focus on pillar (1) technologies for countering cyberattacks. We introduce, in particular, trends in security threats, issues and needs in business, as well as cutting-edge R&D activities to provide solutions [2–4].

2. Solutions in response to customers' security needs

In August 2016, NTT established NTT Security to roll out worldwide consulting and managed security services (MSS). NTT Security brings together security experts, advanced analysis platforms, threat information, and specialized technologies in the NTT Group to gain a competitive advantage and achieve efficient security operations. Since its establishment, NTT Group companies, including Dimension Data, NTT Communications, and NTT DATA have been implementing domestically and internationally total solutions incorporating advanced technologies and services provided by NTT Security.

In the field of corporate risk management, importance is increasingly being placed on OT security measures for securing a business continuity plan in addition to conventional information technology (IT) security measures for protecting information assets. Given these current conditions, NTT Security has started providing security services for defending critical infrastructures such as factories, plants, power systems, and medical institutions. These include (1) consulting services that provide visualization of the components making up an industrial control system and their intrinsic risk, plus associated security measures, and (2) IT/OT integrated security services based on MSS for continuous monitoring of an industrial control network to detect, analyze, and immediately block cyberattacks.



C2 server: C&C (command and control) server
DNS: domain name system
DPI: deep packet inspection
IOC: indicators of compromise
IPS: intrusion prevention system
ISP: Internet service provider
MDR: managed detection and response
WAF: web application firewall

Fig. 2. Dealing with sophisticated and large-scale cyberattacks.

3. R&D of cyberattack countermeasure technologies for increasing competitiveness in security business

Cyberattacks are becoming increasingly sophisticated and large in scale, and more research needs to be done in order to develop technologies to cope with these attacks. At NTT Secure Platform Laboratories, the technologies now being focused on are categorized into *new technology* for providing new countermeasures to security threats and *reinforcing technology* for improving the effectiveness of existing countermeasure technologies. These technologies are outlined in **Fig. 2**.

Up to now, the monitoring targets in the case of defensive security have mostly been corporate and home networks and Internet service provider networks. However, to upgrade countermeasure technologies in order to keep up with the increasingly sophisticated and large-scale cyberattacks, monitoring targets must be expanded to include endpoints and backbone networks, and new technologies must be created with attention given even to the behavior and psychology of users exposed to a cyberattack.

Two examples of new technologies taken up by NTT Secure Platform Laboratories are taint analysis[*1] and forensics[*2]. These are elemental technologies used for generating indicators of compromise, which are used, in turn, as an aid in detecting endpoint infections and identifying tracks and evidence after an infection.

Additionally, analyzing flow[*3] in the backbone network will make it possible to detect a botnet master and infer the server group making up a botnet. This technology will enable security threats to critical infrastructures to be dealt with appropriately.

It will also become possible to detect elaborately designed cyberattacks that depend on user behavior and psychology through a new technique called *usable privacy and security* that has recently become a topic of interest worldwide. This technique, which is the outcome of interdisciplinary research not restricted to technology, efficiently achieves security and privacy protection together with high usability.

[*1] Taint analysis: A technique for analyzing the dependency between data by propagating a tag set in an item of data according to rules.

[*2] Forensics: Analysis of digital information and techniques for doing so with the aim of uncovering the causes of an incident, discovering evidence, etc.

[*3] Flow: A session identified by the combination of TCP (Transmission Control Protocol), UDP (User Datagram Protocol), or ICMP (Internet Control Message Protocol) destination/source Internet protocol addresses and port numbers.

References

[1] "Feature Articles: Security Concerns—Growing Threats and Business Opportunities," NTT Technical Review, Vol. 15, No. 5, 2017.
https://www.ntt-review.jp/archive/2017/201705.html

[2] S. Konno, "Collecting, Analyzing, and Leveraging Threat Intelligence at NTT-CERT," NTT Technical Review, Vol. 16, No. 5, 2018.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201805fa2.html

[3] K. Matsuda, Y. Nagatake, F. Takeuchi, and K. Yozawa, "Security Business Solutions for Customer Needs," NTT Technical Review, Vol. 16, No. 5, 2018.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201805fa3.html

[4] T. Hariu, D. Chiba, M. Akiyama, T. Yagi, Y. Kawakoya, Y. Nagafuchi, and T. Koyama, "Cyberattack Countermeasure Technology to Support NTT's Security Business," NTT Technical Review, Vol. 16, No. 5, 2018.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201805fa4.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, MA, 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 cyberattacks, and conducting R&D of technology that can strengthen our competitive edge by ensuring information can be used securely in businesses facing new threats.