R&D on Security Contributing to Creation of New Value

Shinichi Hirata

Abstract

NTT Secure Platform Laboratories is engaged in research and development of security technologies required for a *smart world*. In this article, an information sharing platform of secure data utilization required for a smart world is described, and the efforts of NTT Secure Platform Laboratories to support that world are introduced from two aspects: security that protects the smart world and security that creates the smart world.

Keywords: data utilization, cryptography, security operation

1. The *smart world*

As typified by the key phrase *digital transformation*, digital data are being used by people in various real-world settings, e.g., social activities, and the way people live their lives and work is changing rapidly.

A large amount of digital data is acquired from physical spaces and used in various settings concerning social activities. Our aim to make use of digital data is threefold: (i) process this large amount of data in cyberspace in sophisticated ways, return the data to the physical space, and use them there; (ii) make it possible for all people to live safely and in their own way through those data-related activities; and (iii) enable society to work smoothly. We call this world view a *smart world*. It is assumed that a smart world will enable two types of optimization: *personal optimization*, namely, fulfilling safe and healthy living through a personalized and customizable living environment, and *social optimization* such as creating industrial systems that can achieve total optimization based on forecasts and work environments that are suitable for the requirements of workers (i.e., work hours, places, etc.). We are striving to create security technologies necessary for safe and secure use of large amounts of digital data, which is indispensable for a smart world.

2. Recent trends in security

Society has started to make the major changes needed to achieve a smart world; however, should we not determine the nature of threats present in today's cyberspace before achieving this?

In information technology (IT), the following threats are noteworthy: business-email compromise (BEC), namely, stealing management information from a company using email, etc. and exploiting that information to threaten or defraud people or businesses; supply-chain attacks targeting vulnerable parties (customers, contractors, etc.) in the product lifecycle (design, manufacture, use, and disposal) of information devices; and activation of fake news exploiting social networking services.

BEC involves attackers who infiltrate corporate-information systems and spoof corporate transactions and management information. In particular, an attack attempts to steal money or confidential information of a company by impersonating the compromised company and exchanging fake information with related parties such as customers of the compromised company.

According to a report by the FBI Internet Crime Complaint Center released in April 2019, there were 351,937 BECs in the USA in 2018 (up 17% from the previous year), and the damage amounted to $2.7 billion (up 46% from the previous year) [1]. Moreover,

as an attack that attempts to steal confidential information from systems and networks and stop certain functions, a supply-chain attack penetrates the product-design, manufacturing and distribution processes then distributes hardware, firmware, software, etc. that can attack third parties throughout the market. It has become clear that such attackers have successfully distributed firmware and software, including backdoors, to commercially available personal computers and smartphones.

In operational technology (OT) (i.e., control networks) and the Internet of Things (IoT), the number of attacks on critical infrastructure has increased. These attacks target control networks operating inside public facilities that support people's lives (such as electric, gas, water, communications, broadcasting, and transportation) by targeting these facilities. Actions that lead to suspension or destruction of these facilities are expected to disrupt the lives of the public, for example, by stopping power transmission from power plants and eventually causing large-scale blackouts. The common trend in the above security-threats is that cyberattacks have recently impaired the security of the general public and nations. In other words, they are evolving into attacks targeting larger victims.

3. Security technologies for protecting a smart world and for creating a smart world

What security technologies must we provide for the coming smart world? We are focusing on two key phrases: *protecting a smart world* and *creating a smart world*. Security technology for protecting a smart world protects various networks and IT systems (such as IT, IoT, and Internet service providers) and users from cyberattacks. Security technology for creating a smart world create a smart world by promoting secure data utilization by applying cryptography and supporting active use of data to activate corporate activities and ensure safe daily living. These two key phrases are positioned as the two pillars holding up our research and development (R&D) on security.

4. Security technology for protecting a smart world

As described above in "Recent trends in security," it is expected that new cyberattack techniques will appear daily and the sophistication and expansion of these attacks will increase. The sophistication and increasing number of cyberattacks increase security risks facing companies and organizations. The elements that make up security risks are broadly divided into threats, vulnerabilities, and assets that companies and organizations should protect. However, even for major companies that value security, the cybersecurity budgets that individual companies and organizations can bear are limited to about 15% of their IT-system budgets, and that figure drops to 5% or less for small and medium-sized companies. To counter the spread of cyberattacks in the future, companies and organizations must drastically improve their ability to defend against and counter cyberattacks (**Fig. 1**).

To improve the defense and countermeasures against cyberattacks, we are developing the following technologies in response to the sophistication of cyberattacks: advanced technology for detecting malware in endpoint devices; advanced technology for determining malicious domains; and technology to counter attacks that exploit the psychological weaknesses of users. We are also developing the following technologies in response to increasing number of cyberattacks: technology for improving operational efficiency and labor-saving technology for security operations [2].

To counter cyberattacks in OT/IoT, under the assumption that various devices (such as IoT and control) are connected, it is necessary to (i) ensure security throughout the supply chain and the product lifecycle (spanning design, manufacturing, distribution, construction, operation, and disposal) and (ii) implement multi-layer measures through cooperation among industrial fields. Under the assumption that IoT is going to be applied, for example, to factories, buildings, agriculture, and monitoring and maintenance systems, we are advancing R&D on authenticity and integrity monitoring technology for IoT devices, which detects software tampering of IoT devices and control devices at the manufacturing, distribution, and operation stages, and cyber physical anomaly detection technology, which detects illegal behaviors during operations. Moreover, in line with advancements in the mobility field, such as sensor networks for cars and autonomous vehicles, we are pushing ahead with R&D on real-time anomaly-detection technology for in-vehicle networks and attack-detection technology on the cloud, which quickly and accurately detect and analyze attacks against vehicles and attacks by vehicles that have malfunctioning in-vehicle networks, as well as fake-sensor-data detection technology, which prevents

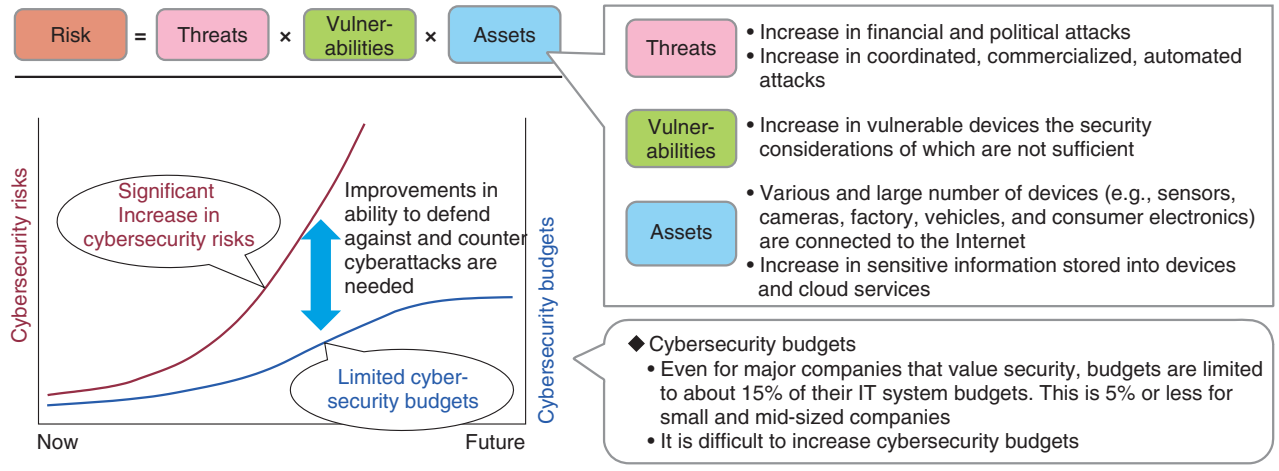

Fig. 1. Cybersecurity risks and budgets.

confusion regarding traffic information due to mixing of false sensor data. In addition to the above-mentioned technologies as countermeasures against cyberattacks on OT and IoT systems, we must develop integrated countermeasures and formulate rules based on the interdependence of IT security, functional safety, and physical security.

5. Security technology for creating a smart world

To create a smart world, it is essential to provide technologies that support safe data distribution and use, namely, solving problems caused by unauthorized use of data, data hoarding, and privacy breaches. These technologies are composed of a flexible and secure data distribution and analysis mechanism that can use data across fields and enable secure execution of all value-creation processes (from data generation, utilization, and analysis to disposal).

Data have thus far been held and used only within a single business entity. However, to create a smart world, the following mechanisms are required: for conducting advanced analysis (integrated analysis) by combining secured data to keep privacy and trade secrets while sharing them between organizations; and for solving various issues and returning the solutions to society on the basis of the results of cross-sector integrated analysis. These mechanisms will enable secure data utilization across industries and fields while creating unprecedented new value (**Fig. 2**).

We are working on secure computation technology to compute a function on encrypted data and anonymization technology that enables safe use of personal data as core technologies to enable such value creation [3]. When analyzing and utilizing data, the data generally have to be decrypted; thus, data utilization related to sensitive data (e.g., trade secrets and personal information) is not progressing. The above-mentioned secure computation technology supports the creation of a world that facilitates solving problems by taking into account the handling of information related to individuals and companies then sharing necessary data between organizations according to the purpose. In September 2019, we announced the world's-first secure computation technology enables model training with a deep neural network while training data are kept secret [4].

Anonymization technology makes it possible to create various anonymously processed information, including data concerning the proprietary technology of NTT Secure Platform Laboratories. With the enforcement of the revised Act on the Protection of Personal Information of 2017 in Japan, if personal information is processed as anonymously processed information, it can be provided to third parties without the consent of the individual. The anonymization technology of NTT Secure Platform Laboratories, which is in compliance with the above act, has been commercialized as anonymously processed information creation software by NTT TechnoCross Corporation.

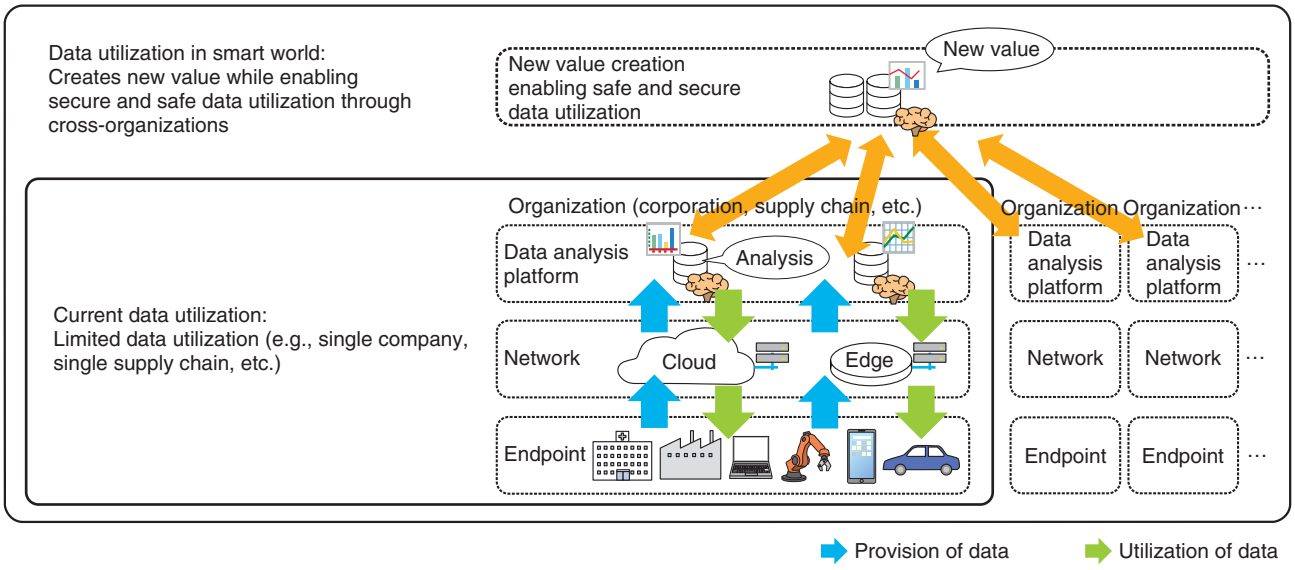

Fig. 2. Data utilization in a smart world.

6. Activities related to Center of Excellence (CoE)

We are actively involved in activities at NTT's CoE with the aim of creating technology that enable the competitiveness necessary for the NTT Group to support a smart world.

Through the activities of the CoE, our highly skilled human resources are taking the initiative in the academic and professional communities. Regarding cybersecurity, we are focusing on management of expert communities and global security contests as well as development of human resources in collaboration with universities. Regarding data security, with an eye on 10 to 20 years from now, we are also researching fully homomorphic encryption, which can be called the next generation of secure computation; post-quantum cryptography, which maintains security even if quantum computing becomes a reality; and quantum computing as the world's-most-advanced research for cryptography [5]. We are also focusing on consulting activities to use the knowledge thus far accumulated at NTT Group companies and supporting the development of safe and secure systems and applications that comply with privacy protection and legal systems.

7. Future developments

As described in this article, NTT Secure Platform Laboratories is engaged in various R&D activities related to security with the aim of becoming the source of the advancement and differentiation of the NTT Group's security technologies while striving to create a safe and secure smart world.

References

[1] Press release issued by FBI, "FBI Releases the Internet Crime Complaint Center 2018 Internet Crime Report," Apr. 22, 2019. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2018-internet-crime-report

[2] M. Iwamura, Y. Kanemoto, Y. Kurogome, K. Aoki, Y. Kawakoya, S. Orihara, and J. Miyoshi, "The Forefront of Cyberattack Countermeasures Focusing on Traces of Attacks," NTT Technical Review, Vol. 18, No. 4, pp. 16–21, 2020. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr202004fa3.html

[3] T. Miyazawa, T. Fukunaga, G. Takahashi, R. Kikuchi, S. Takahashi, and S. Hasegawa, "The Future of Data Distribution and Its Security Technology," NTT Technical Review, Vol. 18, No. 4, pp. 11–15, 2020. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr202004fa2.html

[4] Press release issued by NTT, "Secure Computation for a Typical Training Algorithm of a Deep Neural Network," Sept. 2, 2019. https://www.ntt.co.jp/news2019/1909e/190902a.html

[5] M. Abe, Y. Tokunaga, M. Tibouchi, R. Nishimaki, and K. Xagawa, "Cutting-edge Research on Cryptography Theory in Respond to Changes in Computing Environments," NTT Technical Review, Vol. 18, No. 4, pp. 22–26, 2020. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr202004fa4.html

Shinichi Hirata
Vice President, Head of NTT Secure Platform Laboratories.
He received a B.S. from Hokkaido University in 1990. He joined NTT in 1990 and has been engaged in R&D of cryptography, IC card technology, and authentication systems.