Security R&D Activities for Cloud Services

Toshiyuki Miyazawa, Yosuke Aragane,
Yoshiaki Nakajima, and Hidetsugu Kobayashi

Abstract

The use of cloud services for handling economically and socially important information is increasing. In line with this trend, these services have become attractive targets for cyber attackers and have been exposed to more sophisticated cyber threats. Various efforts are underway at NTT to prevent these evolving cyber threats. In this article, we describe the activities of NTT Secure Platform Laboratories to provide safe and secure cloud services to our customers.

Keywords: security, cloud, R&D plan

1. Introduction

Cloud services, which provide storage and processing functions via the Internet, are becoming increasingly popular because of their economic advantages in reducing provisioning and operational costs as well as the convenience of being able to access them from various environments. As the use of smartphones to access the Internet has become more widespread, cloud services have accordingly provided more sophisticated and useful functions and have become an important infrastructure supporting our economy and society.

The incorporation of cloud services into the infrastructure means that cyber attackers have an appealing new target on the Internet. Additionally, cyber attacks are also a national-level threat that is expected to continue evolving at an accelerated pace. Therefore, implementing security countermeasures and security operations based on advanced research is important in order to protect customers' valuable information against evolving cyber threats and to provide safe and secure cloud services.

2. R&D at the NTT Secure Platform Laboratories

NTT Secure Platform Laboratories engages in research and development (R&D) based on leading-edge research on cryptography and malware analysis to contribute safer and more secure services provided by the NTT Group. Our basic R&D plan is to protect internal systems, the communication infrastructure, and enterprise solutions (**Fig. 1**). We are moving forward with R&D guided by a three-part vision: (1) coping with the most highly evolved attacks, (2) realizing safe and worry-free network use, and (3) creating new business through promoting secure use of information. We have targeted four R&D areas (**Fig. 2**) in order to achieve this R&D vision.

2.1 Information security platform

In the area consisting of the information security platform, we conduct leading-edge research on cryptography and develop security technologies that can protect systems and information from cyber attacks and internal fraud and also promote secure use of information. Typical technologies in this area include intelligent cryptosystems and secure computation. Secure computation technology and its evolved form, fully homomorphic encryption, are particularly suited for statistical processing, database processing, and similar types of computation while maintaining the secrecy of data stored in the cloud. The implementation of such techniques can promote not only the use of cloud services but also the creation of new business

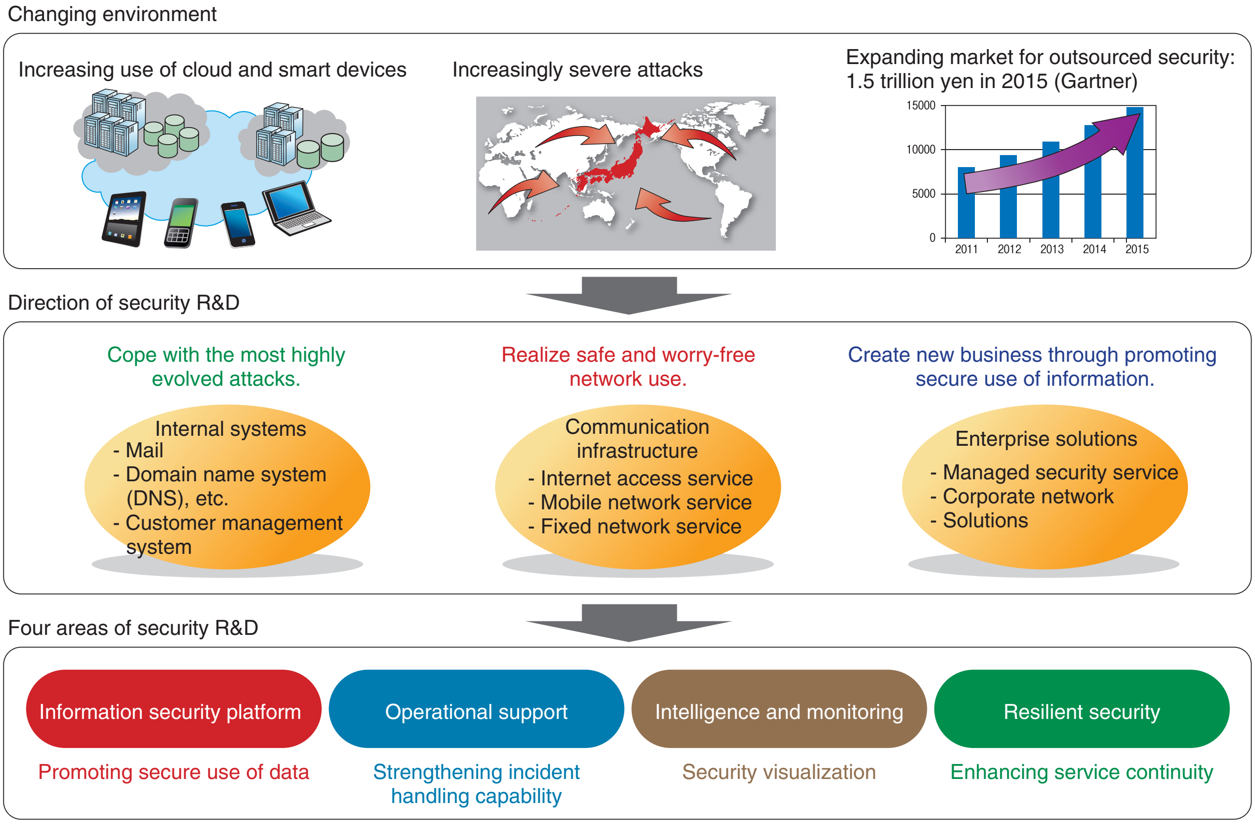

Changing environment
Increasing use of cloud and smart devices
Increasingly severe attacks
Expanding market for outsourced security:
1.5 trillion yen in 2015 (Gartner)
15000
10000
5000
0
2011
2012
2013
2014
2015
Direction of security R&D
Cope with the most highly evolved attacks.
Internal systems
- Mail
- Domain name system (DNS), etc.
- Customer management system
Realize safe and worry-free network use.
Communication infrastructure
- Internet access service
- Mobile network service
- Fixed network service
Create new business through promoting secure use of information.
Enterprise solutions
- Managed security service
- Corporate network
- Solutions
Four areas of security R&D
Information security platform
Promoting secure use of data
Operational support
Strengthening incident handling capability
Intelligence and monitoring
Security visualization
Resilient security
Enhancing service continuity

Fig. 1. Basic plan for security R&D.

that requires the use of sensitive data such as management data and personal information. The activities in this area are described in detail in the articles “R&D on Secure Computation Technology for Privacy Protection” [1] and “Fully Homomorphic Encryption over the Integers: From Theory to Practice” [2] in these Feature Articles. For information on other technologies we are working on, please see Fuji et al. [3].

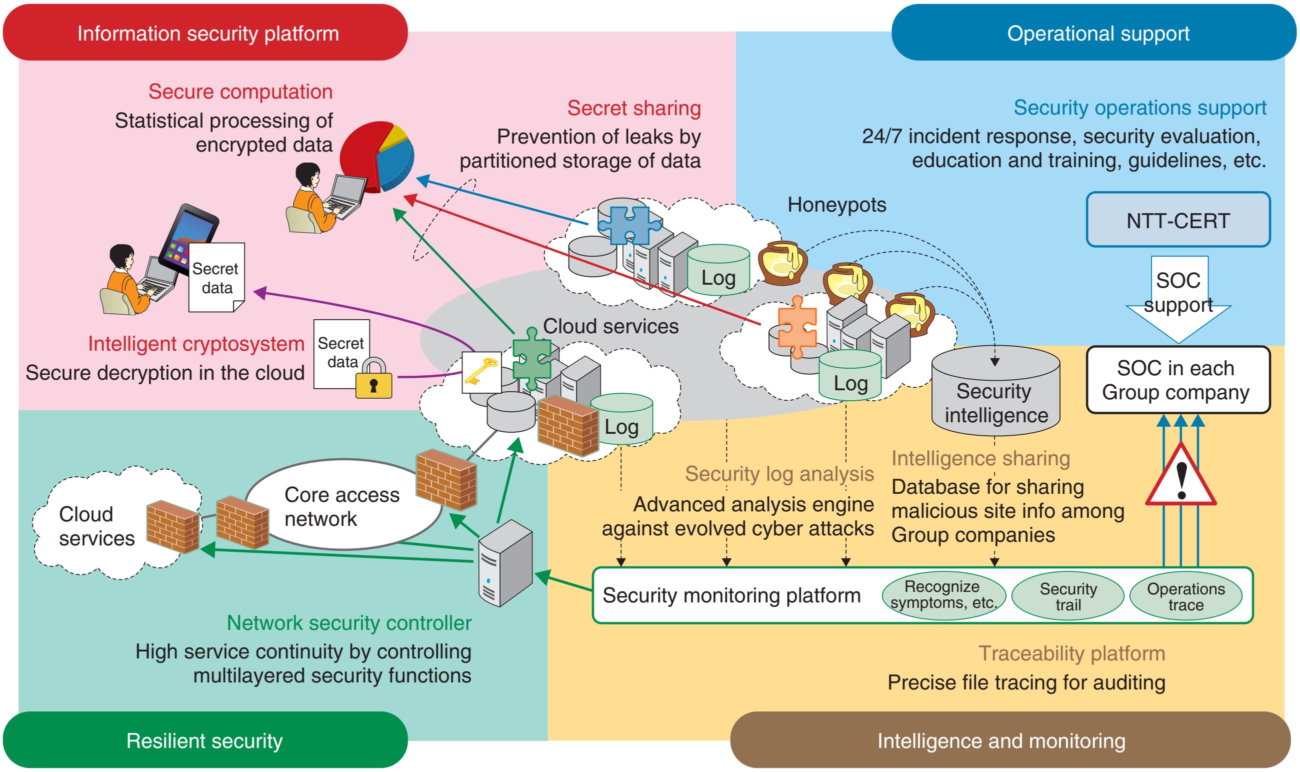
2.2 Operational support

Our R&D in the area of operational support involves supporting security operations of NTT Group companies and improving the technology for such support. Preventing all cyber attacks is difficult because they are constantly evolving. NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team), the CSIRT[*1] organization of the NTT Group, supports security operations in both pre-incident and post-incident measures in order to respond rapidly to cyber attacks on various systems such as the cloud service system, and to minimize the damage of those attacks. For more information on the work of NTT-CERT, refer to Tanemo et al. [4].

2.3 Intelligence and monitoring

The area consisting of intelligence and monitoring involves security visualization technologies that enable early detection of cyber attacks and provide an accurate understanding of the system status. In order to achieve early detection of cyber attacks, we research and develop technology for security log correlation analysis and malware analysis. We are also gathering information on malicious sites that infect and distribute malware and are providing such information as security intelligence to NTT Group companies. For more information on this work, please see Hariu et al. [5]. Security threats can also arise from internal fraud and operation errors, so it is important

[*1] CSIRT (Computer Security Incident Response Team): An organization responsible for incident response in the broad range of preventing cyber threats, detecting cyber attacks, and handling security incidents.


Information security platform
Operational support
Secure computation
Statistical processing of encrypted data
Secret sharing
Prevention of leaks by partitioned storage of data
Security operations support
24/7 incident response, security evaluation, education and training, guidelines, etc.
Honeypots
NTT-CERT
SOC support
Secret data
Intelligent cryptosystem
Secure decryption in the cloud
Secret data
Cloud services
Log
Log
Log
Security intelligence
SOC in each Group company
Cloud services
Core access network
Security log analysis
Advanced analysis engine against evolved cyber attacks
Intelligence sharing
Database for sharing malicious site info among Group companies
Security monitoring platform
Recognize symptoms, etc.
Security trail
Operations trace
Network security controller
High service continuity by controlling multilayered security functions
Traceability platform
Precise file tracing for auditing
Resilient security
Intelligence and monitoring

SOC: security operation center

Fig. 2 Security R&D overview.

to accurately comprehend the information flow within the system in order to maintain security. Visualizing the information flow is especially important with cloud services; such visualization makes it possible to strengthen the security of cloud services and to increase the sense of trust that customers have in cloud providers. In these Feature Articles, we introduce R&D on "The TRX Traceability Platform," which enables visualization of the information flow by collecting and linking various event logs from cloud services and other services [6].

2.4 Resilient security

Resilient security is a new area of R&D. A resilient function can avert a complete service shutdown and restore the service to a normal state, even when the service is affected by cyber attacks or natural disasters. To achieve cloud services with this resilient function, we are working on autonomous recovery technology that enables cooperation and control of virtual network technology and virtual appliance technology. The concept and component technologies of resilient security are described in the article "Resilient Security Technology for Rapid Recovery from Cyber Attacks" [7] in these Feature Articles.

3. Future study

Security is relevant to a very broad range of areas, and some of them are beyond the scope of our laboratories. In the four areas of our R&D described above, cooperation with global organizations is important. In particular, we cooperate closely with NTT I^3 (NTT Innovation Institute Inc.), an R&D facility in North America, by sharing the latest needs in the North American market and advanced technological knowledge in the cloud and security fields. We will proceed with security R&D to achieve our vision through cooperation with internal and external organizations.

References

[1] K. Chida, D. Ikarashi, T. Miyata, H. Takiguchi, and N. Kiribuchi, "R&D on Secure Computation Technology for Privacy Protection," NTT Technical Review, Vol. 12, No. 7, 2014.

https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201407fa4.html

[2] M. Tibouchi, "Fully Homomorphic Encryption over the Integers: From Theory to Practice," NTT Technical Review, Vol. 12, No. 7, 2014.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201407fa5.html

[3] H. Fuji, A. Fujioka, T. Kobayashi, K. Chida, F. Hoshino, T. Miyazawa, and K. Suzuki, "Cryptographic Techniques that Combine Data Protection and Ease of Utilization in the Cloud Computing Era," NTT Technical Review, Vol. 10, No. 10, 2012.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa3.html

[4] 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

[5] T. Hariu, M. Akiyama, K. Aoki, T. Yagi, M. Iwamura, and H. Kurakami, "Detection, Analysis, and Countermeasure Technologies for Cyber Attacks from Evolving Malware," NTT Technical Review, Vol. 10, No. 10, 2012.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201210fa2.html

[6] T. Motoda, T. Nagayoshi, J. Akiba, and K. Takeuchi, "The TRX Traceability Platform," NTT Technical Review, Vol. 12, No. 7, 2014.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201407fa2.html

[7] T. Koyama, K. Hato, H. Kitazume, and M. Nagafuchi, "Resilient Security Technology for Rapid Recovery from Cyber Attacks," NTT Technical Review, Vol. 12, No. 7, 2014.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201407fa3.html

Toshiyuki Miyazawa

Senior Research Engineer, Information Security Project, NTT Secure Platform Laboratories.

He received the B.E. and M.S. in mathematics from Waseda University, Tokyo, in 2000 and 2003, respectively. Since joining NTT Information Sharing Platform Laboratory in 2003, he has been engaged in R&D of information security, especially of public key cryptography and security protocols. From 2008 to 2011, he was with the IT Innovation Department at NTT EAST. He is a member of the Japan Society for Industrial and Applied Mathematics. He received the SCIS Paper Award from the Institute of Electronics, Information and Communication Engineers (IEICE) in 2007.

Yosuke Aragane

Senior Research Engineer, Planning Section, NTT Secure Platform Laboratories.

He received the M.S. and Ph.D. from Tokyo Institute of Technology, Tokyo, in 1997 and 2005 respectively. In 1997, he joined NTT Multimedia Network Laboratories, where he researched human factors and communication management methods in intelligent transportation systems (ITS). Since then, he has been involved in R&D focusing on ITS and security. From 2008 to 2011, he was with the IT Innovation Department at NTT EAST. He is a member of the Institute of Electrical and Electronics Engineers, the Association for Computing Machinery, IEICE, and the Information Processing Society of Japan (IPSJ). He was awarded the Best Paper Award from IPSJ in 2006 and has served as a committee member of major international conferences.

Yoshiaki Nakajima

Senior Research Engineer, Supervisor, Planning Section, NTT Secure Platform Laboratories.

He received the B.S. in information science and the M.S. in mathematical and computing science from Tokyo Institute of Technology, Tokyo, in 1995 and 1997, respectively. In 1997, he joined NTT Information and Communication Systems Laboratories, where he worked on R&D of information security. From 2009 to 2013, he was with the Security Strategy Section of the Technology Planning Department. He has been involved in R&D of information and communication platforms, security platforms, and other areas.

Hidetsugu Kobayashi

General Manager, Human Capital Management Group, NTT Research and Development Planning Department.

He received the B.E. from the University of Tokyo in 1987 and the M.S. in information networking from Carnegie Mellon University, USA, in 1991. Since joining NTT in April 1987, he has contributed to the development of a range of network security related products such as firewalls for IP-VPNs and authentication servers for the NGN. His research interests include network security and information networks. As of July 1, 2014, he moved from NTT Secure Platform Laboratories to NTT Research and Development Planning Department.