2-2 Research and Development of Security Architecture: Overview

Kazumasa TAIRA

We, in the years from FY2011 to FY2015, conducted the research and development (R&D) of security architecture ensuring the secure construction of next-generation networks, following the 3rd Medium- to Long-Term Plan.

In this article, we introduce the overview of our R&D activities.

1 Introduction

For the purpose of realizing the society where everybody can use information and communication networks in a safe and secure way and furthermore without being aware of the security devices that ensure the safety and security of networks, R&D activities aiming for the realization of robust networks against-attack with a high-level of security must be conducted from medium- to long-term perspectives. In particular, among such activities, it is necessary to construct the networks of an architecture employing advanced security technologies—such architecture would be required to ensure the security of different types of network devices or users that are operating or working in different environments through timely and properly providing appropriate security countermesures that are neither excessive nor inadequate.

NICT conducted, in the years from FY2011 to FY2015 of the 3rd Medium- to Long-Term Target Period, the following R&D of security-architecture technologies for the secure construction of next-generation networks: risk-evaluation technologies for ensuring network security; authentication / privacy preserving technologies for resource limited devices used in IoT; and security evaluation techniques for cryptographic protocols in order to keep the security of network-based communications.

In this article, the outline of the above-mentioned R&D projects, which are classified into the following four major categories of research objectives, is introduced.

- R&D of security-knowledge base and its analysis engine

  R&D of the technologies for analyzing security risks existing in the applications on smartphones, the technologies for controlling the security vulnerabilities existing in IT resources preserved in information systems, and the technologies used on the occasions of security information exchanges between organizations.
- R&D of large-scale authentication / privacy preservation

  R&D of the security technologies enabling both authentication and privacy preservation at the same time aiming for implementation in the "resource limited devices," particularly RFID Tags, which are expected to be used in different ways on large-scale networks of IoT era.
- R&D of security architectures for New Generation Networks

  R&D of security architecture, particularly focusing on how to preserve the security and ensure the preservation of privacy in the New Generation Networks expected to hold devices of a 10 trillion-scale number.
- R&D of security evaluation techniques for cryptographic protocols

  R&D of evaluation methods with theoretically completeness for cryptographic protocols, which specify communication procedures of using cryptography, for the purpose of the preservation of the security of the communications on networks, and distribution of the information of the evaluation of major cryptographic protocols.

2 Research and Development Subjects: Overview

As for the above-mentioned R&D subjects, what we have conducted and what achievements we have attained

are presented below. For the details of the individual R&D subjects, the readers refer to the subsections of Section **6** is recommended.

(1) R&D of security knowledge-base / analysis engine

We conducted the R&D for the purpose of establishing the technologies to make evaluations and automatically produce reports on the possible risks when users enjoy services via networks—"knowledge-base" is used for accumulating the information used for the risk evaluation.

At first, we built the "security knowledge-base," for accumulating a variety of security information to be used for taking various types of security countermeasures. Prior to the construction, we conducted the studies on the formal methods for the collection / exchange of security information. At the same time, for the purpose of building the "security-analysis engine," we conducted the studies on analysis methods. The security-analysis engine performs technical analyses; on the other hand the users of systems demand "security" in a different manner. In order to clearly define the user's security requirements, interface the technical security analyses with the user's requirements, and finalize the agreement, the Security Level Agreement (Security SLA) is defined. We developed the description method of such security requirements and protocols to be used for the system-user and the service provide to finalize the agreement.

We have been putting our efforts during this R&D into the construction of the mechanism to automatically make evaluation and report to the users of the threats on the occasions of using smart-phone applications, a need which has recently become a big social issue. We targeted Android applications (hereinafter, referred to as Android apps), proposing and implementing our original method for making evaluation of "threat" and "vulnerability"; as for the evaluation of "threat", the method creates the quantitative evaluation of the possibility that an Android app is a malware using statistical and machine learning techniques according to the context of the Android app downloaded from the Internet; as for the evaluation of "vulnerability," the method make the evaluation by finding the defections in the coding. We accumulated the evaluations and meta-information of about 200,000 Android apps in our security knowledge-base; prior to make the knowledge-base, we determined its information structure and made evaluation.

As for the development of schema required for exchanging incident information conducted in those frameworks, we took the leading role in the Internet Engineering Task Force (IETF) for the international standardization of the technology—the schema came into effect as RFC7203. In addition, we developed a prototype of the automatic vulnerability-alert for enterprise networks using these technology.

During this R&D term, we constructed, by using our knowledge-base, a prototype of the vulnerability control system for IT assets of information systems. The prototype has the following functions; automatically collecting the information of the IT assets on networks; converting such information into IDs; searching the knowledge-base by using the IDs to retrieve vulnerability information, and providing information-system managers with reports / warnings on a real-time basis. During the field study stage of the prototype construction, we received cooperation from the Japan Agency for Local Authority Information System (J-LIS) to conduct interviews of a number of local authorities for actual situations of vulnerability control in its local networks and found out what is needed for vulnerability control. Then, we started the studies on prototype-construction.

(2) R&D of the technologies for large-scale authentication / privacy preservation

We predict that, in the IoT era expected to show increasing advances, a large number of resource limited devices such as sensors will transmit data, which will be added to the conventional traffic. RFID tags, which will be distributed through being attached to everything, currently, do not use encryption for communication due to resource-constraints. Such situations will raise significant issues of authentication or privacy preservation. Therefore, we decided to create safe cryptographic protocols for the purpose of secure communication while also solving the issues of authentication or privacy preservation.

First of all, we constructed the theoretical frame-work of security / privacy preservation requirements for RFID tags. Then, we developed RFID-authentication-protocols that ensure provable safety, and at the same time, we developed a protocol that ensures safe authentication of the RDID owner. Then, regarding the authentication / privacy preserving technologies for RFID, we constructed a protocol that keeps evidences of the event where high-speed read-out actions were carried-out on a number of tags, proposing the protocol that ensures provable high-security against man-in-the-middle attacks (MIMA).

Furthermore, we constructed, by taking advantage of the Physical Unclonable Function (PUF), a protocol of

which the security is physically proven. Through analyzing SRAM PUF behaviors by using 100 FPGAs, we implemented the protocol and obtained the circuit-size and operation-time. Also, we specified a variety of requirements for PUF that are required to prove the security, for the purpose of establishing the scheme for preserving the physical security of resource limited devices.

Then, we conducted the performance evaluation of the privacy preserving authentication protocol for RFID from the practical aspect on the circuit-size, operation-performance, communication-range, and other items by implementing the protocol in the middle of the tag-production process—we conducted the research as contract-research. In addition, we developed a prototype RFID cryptography evaluation circuit-board—expected to help the development of cryptography protocols applicable to wireless-communication environments—, for the purpose of assessing the RFID communication environments from the view of security. We have a plan to collaborate with domestic/overseas hardware developers in the RFID field, for the purpose of providing the prototype boards for the development of the next generation RFID-tags.

On the other hand, we developed the cryptography on which the implementation of a cryptography system satisfying individual sets of requirements is enabled—different application-services available on a large-scale platform have different requirements on security or privacy preservation. Bilinear-map based cryptography have been regarded as the major candidates of the technologies for ensuring privacy preservation. However, questions were raised on the security of some types of such technologies. We have proposed the method for converting such types of cryptography into those that are applicable in a safer manner; the proposed method will, in addition to contributing to the relief of conventional cryptography, provide those that create new methods with a reference standard.

(3) R&D of security architecture for New-Generation Network

Over 10 trillion devices are expected to connect to New Generation Network, and thus such a network will have to provide services to a vast number of users. Such a network is required to have functions not limited to issuing encryption keys but also including revoking keys on the occasions of user-deletion and loss of keys. During the R&D, we conducted the construction of the technologies that will be used for the preservation of security and privacy.

We developed, for the purpose of preserving scalability, a "Revocable ID-based Signature " for the authentication-revocation process of unused devises, which ensures the processing time that will show a log-order increase, as the number of devices grows, implementing its library that is expected to be used in new generation networks. The above-mentioned technology is expected to be effective, particularly, in a disaster situation where many devices stop working, for reducing the operation-cost of authentication. On the other hand, for operating deciphering codes implemented in a system for a long time, key-revocation functions, which will be used on the occasion of exiting the system or key-losses; we proposed the ID based encryption with key-revocation functions, for the purpose of attaining the unprecedented level of security. In addition, we proposed the ID-based encryption where the length of cryptogram is not constrained by the depth of its structure, and the risk of attacks from inside are taken into consideration. Furthermore, we proposed a group-signature scheme where the token-size that is publicized at the time of user-deletion is independent of the number of users.

Regarding privacy preservation, we proposed a system that ensures service-providers authenticate their users without knowing users' real names and at the same time provide their service contents in encrypted form by integrating cryptography —ID-based encryption and group signature—and The Onion Router (Tor). Also, for the purpose of satisfying both privacy preservation and information-utilization, we proposed a system that ensures service-providers protect any part of user's personal information from being revealed on the occasion of purchase-history-leakage and, in an emergency situation, identify the user for tracking; furthermore, aiming for the construction of a encryption system that has a strong safety property without sacrificing convenience, we developed a road-to-vehicle communication system that utilizes time-dependent anonymity. In the system, the key-provocation function for signature was implemented for the purpose of preventing leakage risks on the occasion of car-disposal or key-loss. Furthermore, as for the countermeasure for the occasion of search-token leakage, we proposed a search function that enables deleting tokens.

(4) R&D of the security evaluation techniques for cryptographic protocols

Recently, severe vulnerabilities were found in the communication protocols using cryptography including Service Sockets Layer / Transport Layer Security (SSL / TLS); the organizations providing their services by using

SSL / TLS through the Internet have found great difficulties in taking actions against those vulnerabilities. This situation suggests that such types of vulnerabilities will be possibly found in other communication protocols currently used. Therefore, in this R&D we conducted the vulnerability evaluations of cryptographic protocols used in the Internet and the release of the evaluation results to increase the social awareness of such vulnerabilities.

Furthermore, we found the vulnerabilities and method of fixing for the "Key management protocols" specified in ISO / IEC 11770-2, 3, making a proposal for amendment to ISO / IEC. Our proposal triggered the discussions in ISO / IEC on the amendment of the security definition of the key management protocols specified by ISO / IEC. In addition, regarding the security evaluation methods with theoretical completeness for cryptography protocols, we established a formal method that enables security evaluation in every execution environment. During the evaluations, by examining the methods of new cryptographic protocols proposed by other researches in the most prominent international conferences, we successfully detected the attacks which were not detectable at the time when those protocols were proposed to such international conferences. In addition, using formal methods, we developed a prototype for the visualization system of cryptographic protocols security evaluation, enabling the intuitive understanding of the theoretical completeness of security evaluation, details of attack sequences, and vulnerabilities.

With regard to cryptographic protocols security evaluation, we took the originator role for the establishment of Cryptographic protocol Evaluation toward the Long-Lived Outstanding Security (CELLEOS) Consortium "— a consortium for contributing to society through making discussions from the global standpoint and giving the achievements back to the society. Taking the administrative role to make contributions to the consortium; in addition, we developed the "Cryptographic Protocol Verification Portal (CPVP)" and provided it to CELLOS; and moreover we contributed to the CELLOS's activities for promptly distributing security information and promoting the secure utilization of cryptographic protocols in communication systems, through providing the results of the evaluations we made on the technical validity for the vulnerabilities discovered in SSL / TLS and their possible impacts on actual systems.

We made vulnerability evaluation on the 58 standardized cryptographic protocols including the authentication protocol and added to the results of the evaluation our comments on the possible problems and the technologically reliable information to formulate "AKE Protocol Zoo," publicizing it on the CPVP of the NICT's web-page in October 2015 and making a press release. After the release and announcement, four newspapers reported our announcement (some of the papers reported it on their front pages), and a number of web-sites including "dot." operated by the Asahi-Shimbun Publishing, TECH Ascii, Impress Watch reported it. The portal site received about 9,200 accesses in the week after our announcement and a total of about 35,000 accesses as of the end of March 2016.

(5) R&D of public key system for inter-organization secret communications

We conducted the study, by contract-research, on "Cryptosystems for social organizations," where: as needed, the flexible modification of authority for decryption is ensured. We promoted specific studies on cryptosystems for social organizations, regarding the scenarios of how the cryptosystems are used in actual situations, proposing a number of construction methods of the cryptosystems employable in practical: including operational situations. In addition, in order to clarify the challenges that we will face when operating cryptosystems for social organizations based systems in local authorities, we conducted interview-sessions or technical briefings on such systems in a number of local authorities. Also, by conducting proof-of-concept experiments in a number of local authorities, we clarified, as well as the technical challenges, the challenges for the actual implementation of those systems including user-interface design, operability, and manual description method. In addition, we prepared the implementation standards (guidelines) for the purpose of properly and effectively implementing cryptosystems for social organizations.

3 Conclusions

In this article, the overview of the "Research and development of Security Architecture" conducted in the 3rd Medium- to Long-Term Target Period were introduced. The networks that are currently in operation were implemented on the architecture designed on the assumption that users have good intentions; therefore, particularly with regard to security preservation or privacy preservation, it is not an exaggeration to say that all the countermeasures that have been taken lag far behind the needs of the actual situations. We have been focusing our efforts on the conduction and proposal and preparation of the technolo-

gies for preserving the security of the currently working networks. Also we have been conducting the studies and proposals of the technologies that ensure privacy preservation in the coming IoT era. NICT, in the 4th Medium- to Long-Term Target Period that started in FY2016, will expand the achievements described in this article, in order to establish the technologies that enable taking security measures automatically without human interventions, and also the construction of technologies for the security preservation or privacy preservation for IoT systems.

Acknowledgment

The author expresses here his appreciation to Prof. Akira Kanaoka of Toho University, Mr. Koji Sobataka of NEC Corporation. Also, the author thanks the following staff members engaged in the daily activities in the laboratory; Mr. Shuuhei Yamaguchi; Ms. Yuko Yashiro; Ms. Naoko Takahashi; Ms. Misako Yamaguchi; Ms. Chikako Murai; and Ms. Miyuki Totsuka.

Kazumasa TAIRA, Ph.D. (Eng.)

Director General, Applied Electromagnetic Research Institute/Former: Director General, Network Security Research Institute,
Former: Acting Director of Security Architecture Labratory
Radio Wave Propagation, Electromagnetic Environment, Communication System