Secure Architecture for Critical Infrastructure

Masami Ueno, Shingo Kashima, Yuminobu Igarashi, and Masahiro Hori

Abstract

Recent developments such as the Internet of Things mean that a wide variety of equipment is now being connected to networks. It is feared that this trend could lead to further increases in threats to cybersecurity. At NTT Secure Platform Laboratories, we are working on technology that can be used to protect critical infrastructure networks by investigating security incidents, automating the analysis and handling of incidents, and reducing latent security risks in devices and equipment.

Keywords: critical infrastructure, wide area networks, IoT

1. Introduction

As the Internet of Things (IoT) increases in scale, a growing number of devices are being connected to networks. This number has been predicted to reach 53 billion by 2020 [1]. The increasing quantity of equipment connected to networks poses an increased threat to cybersecurity. For example, there are already reports of online surveillance camera systems and video recorder equipment being infected with malware and incorporated into a botnet that was used to launch cyber-attacks including DDoS (distributed denial of service) attacks on other information technology (IT) services [2, 3]. IT is also being rapidly adopted in various key infrastructures including telecommunications, finance, aviation, rail transport, electricity, and gas with the aim of improving service quality and reducing costs, and several cases have been identified where this increased dependence on IT has adversely affected infrastructure services due to system failures [4–6].

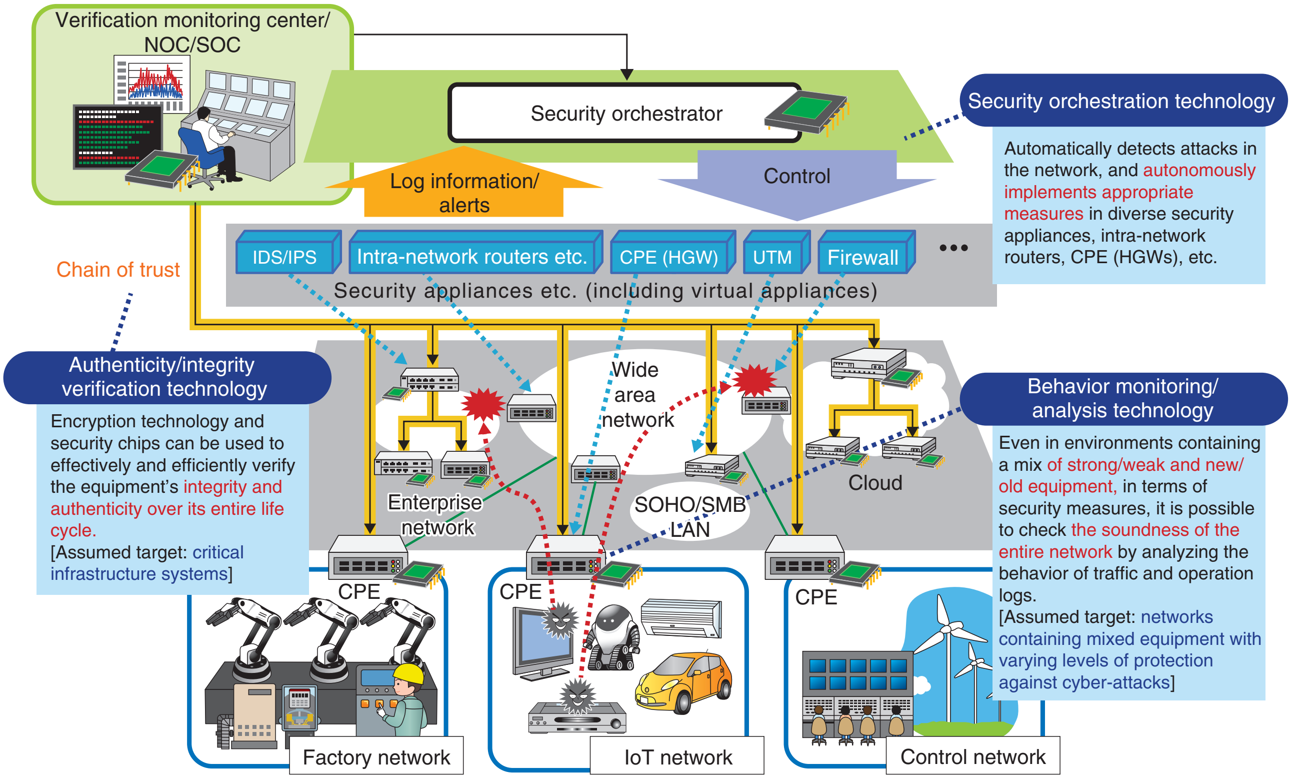
Thus, even critical infrastructure networks are having to face increased threats due to the growing quantity of equipment connected to them, and countermeasures should be discussed urgently. This article discusses security countermeasures that can protect diverse kinds of key infrastructures from cyber-attacks, focusing in particular on the wide area networks[*1] that form part of the key infrastructure used by the communication industry.

2. Wide area network security

Traditionally, the security of a network is maintained by defining a secure zone where a security policy is enforced, and a non-secure zone where security may not be enforced, and by taking steps to protect the secure zone at the boundary between the two zones. Even in wide area networks, when seen from the viewpoint of the network provider, the facilities run by the network operator can be assumed to constitute a secure zone where security is adequately enforced, while the client-side facilities that lie beyond the customer premises equipment (CPE)[*2] such as home gateways (HGWs) and corporate routers are assumed to be a non-secure zone because they cannot be managed by the network operator, and their reliability cannot be assured. At the boundary between the CPE and network operator equipment, a

[*1] Wide area network: General term for a network with a broader reach than a local area network (LAN), which would typically be used by a single organization. Specific examples include networks that use leased lines to interconnect geographically distant LANs, and virtual private networks built on the Internet.

[*2] CPE: Equipment installed at the premises of an Internet service client in order to connect to the network.



Automatically detects attacks in the network, and autonomously implements appropriate measures in diverse security appliances, intra-network routers, CPE (HGWs), etc.

Encryption technology and security chips can be used to effectively and efficiently verify the equipment's integrity and authenticity over its entire life cycle.
[Assumed target: critical infrastructure systems]

Even in environments containing a mix of strong/weak and new/old equipment, in terms of security measures, it is possible to check the soundness of the entire network by analyzing the behavior of traffic and operation logs.
[Assumed target: networks containing mixed equipment with varying levels of protection against cyber-attacks]

IDS: intrusion detection system
IPS: intrusion prevention system
NOC: network operation center
SMB: small- and medium-sized businesses

SOC: security operation center
SOHO: small office home office
UTM: unified threat management

Fig. 1. Security technology research and development.

gateway device such as an edge router is installed so that the security of the network can be assured on a per-circuit basis.

In the future, however, since developments such as IoT will lead to further increases in the amount of equipment connected to client-side facilities, it is envisaged that traffic will need to be controlled by CPE devices situated closer to this equipment.

3. Mechanisms for protecting the security of a wide area network

To maintain the security of a wide area network and take prompt measures when any sort of incident such as an infection or attack has occurred, it is necessary to have mechanisms that can detect incidents, determine what countermeasures to apply to the detected incidents, and then implement these measures. Although the response mechanism for major security incidents is the same as the conventional approach, safeguarding the security of a wide area network in today's changing environment requires CPE devices that detect and deal with incidents in equipment in the non-secure zone while cooperating with mechanisms inside the secure zone. Since the CPE devices are situated at the boundary of the secure and non-secure zones, it is essential to take steps to mitigate their inherent risks (latent defects and misconfigurations, malware illegally embedded prior to shipment, etc.) and physical risks (illegal replacement of components, etc.).

In the following sections, we describe the technologies for behavior monitoring/analysis, security orchestration, and authenticity/integrity verification that are being researched and developed at NTT Secure Platform Laboratories to address these issues (**Fig. 1**).

4. Behavior monitoring/analysis technology

Intrusion detection systems (IDS) and intrusion prevention systems (IPS)[*3] are two examples of intrusion detection mechanisms for the protection of IT equipment. However, these systems are mainly targeted at personal computers and servers, and there are currently only a few products compatible with critical infrastructure systems or IoT equipment. In particular, IoT equipment and the control/monitoring equipment used in critical infrastructures and factories are typically deployed over a wide area and connected to the network in very large numbers, and they operate autonomously and unattended in a wide variety of environments. This differs significantly from the configuration of traditional IT equipment. Furthermore, since IoT equipment is often designed and produced for a specific application, it can be difficult for the equipment itself to implement security measures due to issues such as the equipment having limited functions or performance (equipment with security weaknesses), or being used continuously for long periods without regular security updates (old equipment).

To address this issue, we are researching behavior monitoring/analysis technology aimed at promptly ascertaining signs of security deterioration in the overall health of the system by detecting abnormal behavior in peripheral network equipment. More specifically, we are researching an anomaly detection technique whereby CPE devices such as HGWs placed at the perimeter of a non-secure zone are used to gather statistical information from the communication traffic and operating logs of old equipment or equipment with low security levels for which it is difficult to implement individual security measures. This information is used to construct an analysis model that represents the healthy state of a system containing the characteristics and usage patterns of the equipment, from which it is possible to discover behavior that departs from the normal (healthy) behavior exhibited.

5. Security orchestration technology

For the analysis and handling of detected incidents, most security product vendors provide products where the detection and control functions are linked by proprietary security appliances and the like, but these only work with the vendor's own products, or with the products of certain affiliated companies.

At NTT Secure Platform Laboratories, we are developing security orchestration technology as a vendor-agnostic framework for the automation and semi-automation of security operations that can link together the detection and analysis functions of diverse security equipment, and we are making it available to NTT Group companies. We have developed this as technology that cooperates with the operation of office security appliances and datacenters where there have been clear security vulnerabilities. As further developments in IoT are achieved in the future, we intend to expand the technology to orchestration including CPE devices such as HGWs. For example, by restricting the sources and destinations of traffic through the use of resources such as a pre-prepared whitelist for IoT devices that transmit data to few destinations, it is possible to implement traffic control on a per-equipment basis such as restricting or blocking the flow of traffic when an issue has arisen.

6. Authenticity/integrity verification technology

Security devices that perform detection and control functions are typically placed in the non-secure zone together with CPE devices. If the degree of confidence can be increased by reducing the latent risks and physical risks of these devices, then even if an incident does occur, it will be possible to deal with it more promptly.

At NTT Secure Platform Laboratories, we are working to increase the reliability of these devices and the equipment connected to them by researching a technique for reliably identifying the controlled equipment (authenticity verification) and a technique for confirming the correctness of software running in this equipment (integrity verification).

6.1 Authenticity verification

The purpose of our authenticity verification technique is to confirm that the control and communication equipment itself is operating correctly and is not being spoofed. This is done by designating a dedicated server node as the *root of trust*, and constructing a chain of relationships (trust links) from tamper-resistant components that extend this root of trust out to each item of equipment. Cryptography is used in this chain to authenticate the equipment, thereby confirming the authenticity of the system as a whole. The tamper-resistant components used here have

[*3] IDS/IPS: The detection of fraudulent activity from outside the targeted IT system or network, or a defense system that performs such detection.

mechanisms that are very difficult to analyze externally or extract data from without authorization, and are therefore able to handle cryptographic keys safely.

6.2 Integrity verification

The purpose of integrity verification is to confirm that the software and data in control and communication equipment have not been tampered with. This is done by checking that the software in the equipment matches the correct values stored in tamper-resistant components based on the chain of trust established by the authenticity verification technology. Integrity verification has the advantage of ensuring scalability for the entire system and takes the entire software life cycle into account.

7. Future prospects

We have introduced countermeasures for wide area networks in order to protect the security of key infrastructures in situations where the amount of equipment connected to the network is expected to increase dramatically. Dealing promptly with the occurrence of any incident such as an infection or attack requires a mechanism for analyzing the incident and deciding what countermeasures to use, a mechanism for deploying these countermeasures, and a mechanism for reducing the inherent and physical risks of the equipment. At NTT Secure Platform Laboratories, we are working to address these needs with behavior monitoring/analysis technology, security orchestration technology, and authenticity/integrity verification technology. These technologies can be used not only in wide area networks but anywhere IT has been introduced to keep up with communication trends. In the future, we plan to make this technology applicable to many more areas including critical infrastructure systems.

References

[1] Ministry of Internal Affairs and Communications, “2015 White Paper on Information and Communications in Japan,” Chapter 5: ICT and the Future of Industry, Section 4, 2016.
http://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2015/chapter-5.pdf#page=13

[2] B. Krebs, “DDoS on Dyn Impacts Twitter, Spotify, Reddit,” Krebs on Security, 2016.
https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/

[3] T. Spring, “BASHLITE Family of Malware Infects 1 Million IoT Devices,” 2016.
https://threatpost.com/bashlite-family-of-malware-infects-1-million-iot-devices/120230/

[4] Government of Japan, “The Basic Policy of Critical Information Infrastructure Protection (3rd Edition),” May 19, 2014, Information Security Policy Council; May 25, 2015 (Revised), Cybersecurity Strategic Headquarters.
http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3_r1.pdf

[5] National Center of Incident Readiness and Strategy for Cybersecurity, “Report on IT Dependency Based on Change in Critical Information Infrastructure,” 2015 (in Japanese).
http://www.nisc.go.jp/inquiry/pdf/itizon_gaiyou.pdf

[6] InfoCom Research, Inc., “Report on IT Dependency Based on Change in Critical Information Infrastructure,” 2015 (in Japanese).
http://www.nisc.go.jp/inquiry/pdf/it_izon_honbun.pdf

Masami Ueno

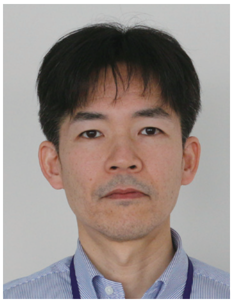
Senior Research Engineer, Secure Architecture Project, NTT Secure Platform Laboratories.

He received a B.E. and M.E. in computer science from Yamanashi University in 1991 and 1993. In 1993, he joined NTT Software Laboratories. He has been engaged in requirement engineering and development of a billing platform and digital rights management system. Since April 2012, he has been conducting research and development (R&D) on security orchestration technology. He is a member of the Information Processing Society of Japan.

Shingo Kashima

Senior Research Engineer, Secure Architecture Project, NTT Secure Platform Laboratories.

He received a B.S. and M.S. in computer science from Kyushu University, Fukuoka, in 2002 and 2004. Since joining NTT in 2004, he has been engaged in R&D of Ethernet virtual private networks, traffic monitoring techniques, and network security.



Yuminobu Igarashi

Senior Researcher, NTT Secure Platform Laboratories.

He received an M.S. in energy science from Tokyo Institute of Technology in 1994 and an M.S. in management of innovation and technology from University of Sussex, UK, in 2009. He joined NTT in 1994 and has been involved in the research and operation of virtual private networks. His current research interests are anomaly detection of IoT networks and devices. He is a member of the Institute of Electronics, Information and Communication Engineers.

Masahiro Hori

Senior Research Engineer, Secure Architecture Project, NTT Secure Platform Laboratories.

He received a B.E. in electrical engineering and an M.E. in information engineering from Kyushu University, Fukuoka, in 1986 and 1988. He joined NTT Software Laboratories in 1988 and studied object-oriented design methods, electronic money technology, and security for e-Government. He joined NTT Secure Platform Laboratories in 2012. He is currently studying a technique to confirm the correctness of software.