Featured Articles II

IoT Security

IoT System Security Issues and Solution Approaches

Shinsuke Tanaka
Kenzaburo Fujishima
Nodoka Mimura, Dr. Eng.
Tetsuya Ohashi
Mayuko Tanaka

OVERVIEW: By connecting various devices to a network and enabling data gathering and analysis, the IoT is expected to contribute to the creation of new customer value. Critical infrastructure that affects people's lives and economic activities will also become an area in which the IoT is used, so security measures for IoT systems are very important. On the other hand, a dramatic increase in the number of connected devices will create technical problems such as attacks with a broader scope of influence and attacks that last longer. So, a shortage of security operations administrators will also be a problem. This article focuses on availability, which is one of the key requirements for IoT security for critical infrastructure. The article presents approaches for proceeding quickly from problem detection to provisional measures to ensure availability, and detection technology developed by Hitachi that has high sensitivity and a low rate of false positives.

INTRODUCTION

WITH the recent spread of the Internet of Things (IoT), the number of network-connected devices is increasing dramatically. The connected devices are not limited to information devices. They comprise an increasingly diverse list of items, including life-related items such as vehicles and medical equipment, and items with potentially large impacts on society such as power stations and nuclear facilities.

Since the IoT consists of various network-connected devices, when one device is infiltrated by malware, it can become the starting point for the spread of the infiltration to other devices that could ultimately threaten critical infrastructure that should ordinarily be protected. Actual past security incidents have demonstrated that vulnerabilities in the communication software of devices connected to critical infrastructure such as work-use personal computers (PCs) and surveillance cameras have been targeted to enable unauthorized access from outside. These devices have been used as starting points for making critical infrastructure operate abnormally[(1)].

This article looks at the security issues involved in adopting the IoT, along with approaches for resolving these issues.

IoT SYSTEM FEATURES AND SECURITY ISSUES

Devices that previously had no communication functions are being connected to a network by IoT systems. These systems enable the discovery of phenomena that were previously unseen, providing new insights. When data gathered from connected devices is analyzed, new knowledge can be acquired. These features make the IoT a promising tool for increasing efficiency by reducing costs or increasing sales. However, in its discussion of security threats in the IoT era, the IoT Acceleration Consortium (a collaborative program with members from industry, academia, and the government) has underscored the need for measures to handle the following three issues: (1) the increasing number of network-connected IoT devices, (2) long life cycles, and (3) the difficulty of perfect manual surveillance[(2)].

In the discussion of the first issue, the increasing number of potential targets for attacks due to the increase in number of IoT devices, as well as the growing scope of influence of attacks have been pointed out. In the discussion of the second and third issues, it has been pointed out that IoT systems require little human involvement, so they can easily lapse into

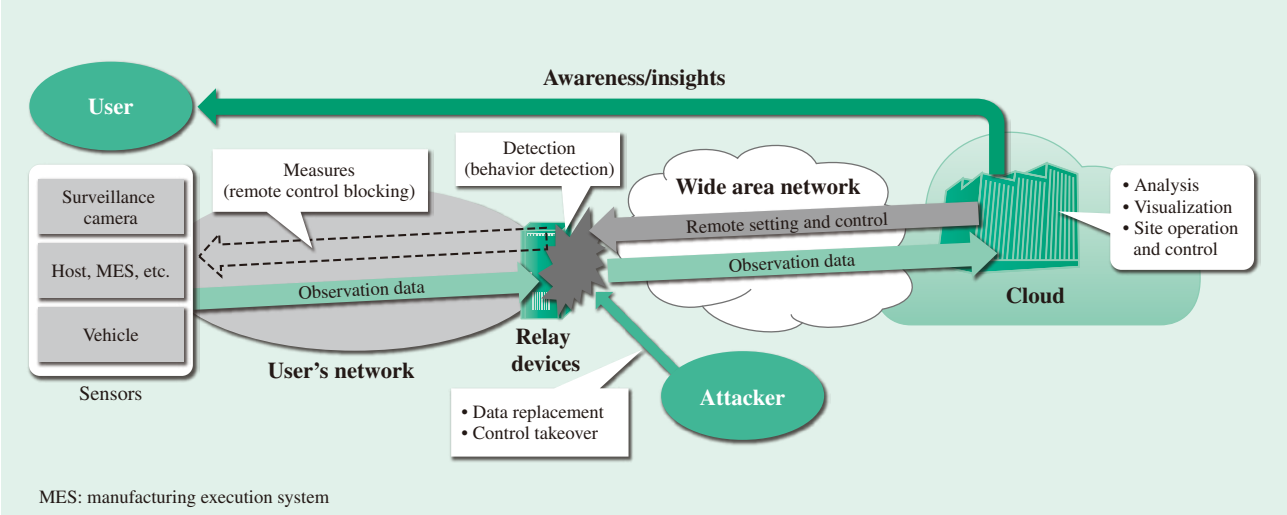

Fig. 1—Layered Architecture of an IoT System.
Relay devices are installed between the sensors and the cloud, and sensor information is gathered by the relay devices. Sensor problems are detected by the relay devices.

a situation where there is a shortage of administrators that makes attack detection difficult, and that long life cycles, over 10 years long, result in attacks that continue for long periods of time. The approaches that Hitachi has conceived to resolve these issues are described below.

APPROACHES TO RESOLVING ISSUES

To respond to the increase in network-connected IoT devices, Hitachi has adopted a layered architecture with relay devices installed between sensors and the cloud. These relay devices are used to gather large volumes of sensor information (see Fig. 1). They can take a variety of forms, such as gateways, switches and routers, depending on the client system.

When responding to the issues of long life cycles and the difficulty of manual surveillance, the two key points are: detecting problems as soon as they occur, and taking provisional measures to prevent the spread of damage while the system continues to operate.

Importance of Immediate Detection

Fig. 2 illustrates the importance of immediate detection using a model for calculating the cost of IoT security damage.

Security damage consists of direct damage and indirect damage. Direct damage includes the primary damage caused directly by the incident (the labor and equipment repair costs needed to handle the incident), and the profits lost due to equipment shutdown. Indirect damage includes the secondary damage caused by the spread of damage such as payment of compensation, damage caused by rumors, and loss of public trust.

Unlike incidents in information technology (IT) systems, incidents occurring in IoT systems can take several months to be discovered. When an incident occurs, the primary damage first starts increasing. Subsequently, the incident is discovered at time t_1, the cause is identified and then provisional measures are taken at time t_2, and finally the system is restored at time t_3. The secondary damage continues increasing

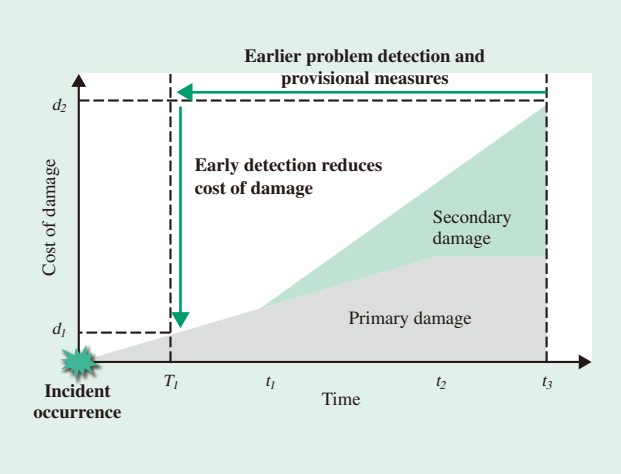

Fig. 2—Model for Calculating Cost of IoT Security Damage.
The cost of IoT security damage is the sum of the cost of the primary damage caused directly from the incident occurrence, and the cost of the secondary damage that occurs as the damage spreads. Carrying out problem detection and provisional measures at time T_1 can reduce the cost of the damage.

for a while after the provisional measures are carried out at time t_2. So, if problem detection and provisional measures can be carried out at time T_1 ahead of the natural discovery time t_1, the cost of the damage can be reduced from d_2 to d_1. The technology required for immediate detection is described in the next chapter.

Requirements for Provisional Measures

Provisional measures are needed immediately after problem detection. The methods used for provisional measures include isolating the location where the incident occurred, defending against further attacks, and reducing damage. Unlike IT systems, critical infrastructure systems often cannot be shut down when incidents occur, so the availability of the entire system must be the top priority when handling incidents.

Incident handling also requires business knowledge of the client systems that use the IoT, such as production lines and power systems. In other words, the same incident can require different handling measures for different systems, and customization involving thorough knowledge of how the client systems work.

Process Flow from Problem Detection to Provisional Measures

This section outlines the methods used to enable early problem detection and rapid provisional measures to ensure the availability of critical infrastructure.

For known problems with previously-created response methods, the process flow from problem detection to provisional response measures can be automated to enable rapid handling and ensure availability.

However, since there are no previously-created response methods for unknown problems, causes must be identified by means such as log analysis, response measures must be proposed for eliminating the causes, and the effectiveness of the proposed measures must be verified. The process flow from problem detection to provisional response measures, therefore, takes time. An effective way to shorten this time is to investigate response measures for hypothetical problems in advance, verify their effects, and create a manual of provisional response procedures.

Approach to Implementing Provisional Response Measures

If damage from incidents such as malware infiltration is expected to spread, one effective way to avoid the worst-case scenario (a complete system shutdown caused by the spread of damage) is to temporarily isolate only the location where the problem occurred from the system (as a provisional measure). To minimize the scope of the temporary isolation resulting from this provisional measure, the problem detection resolution should ideally have at least the same granularity as the isolation. The entire system should therefore be observed in overview to determine the scope of isolation of the location where the problem occurred.

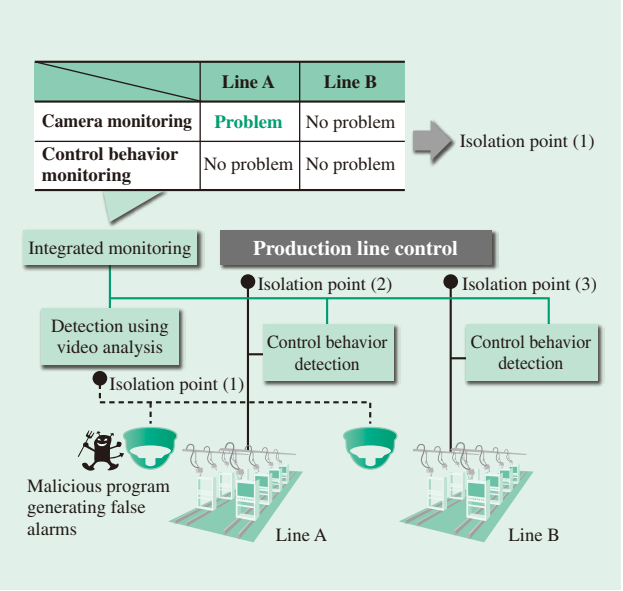

Fig. 3—Behaviors when Detecting Problems on Production Lines. The example above illustrates how two production lines can be monitored using a camera and control behavior to detect and isolate problems.

As an example, Fig. 3 illustrates how the behavior of two production lines (line A and line B) can be monitored by two methods—camera monitoring and control behavior monitoring.

First, consider a situation in which a malicious program is introduced into the camera for line A and generates false alarms indicating problems in line A. In this case, there is no problem with the control of line A itself, so the system is isolated at isolation point (1) to prevent the spread of damage. However, if a problem is found in both the camera and the control behavior of line A, then a problem in line A itself is deemed to have occurred, so the system is isolated at isolation point (2).

Creating a manual beforehand that specifies how to isolate the system depending on the nature of the problem in this way makes it possible to create provisional measures based on business knowledge. The provisional measures specified in this manual can then be implemented as programs at the isolation points, enabling them to be automated.

This method and the detection technology presented in the next chapter can be combined to enable the process from problem detection to provisional measures to be accomplished as rapidly as possible.

TECHNOLOGY FOR IMMEDIATE DETECTION

The security of critical infrastructure networks has conventionally been ensured by isolating the networks from the outside. However, these networks are becoming integrated with information networks to enable business innovation, and recently there have been demands to connect them to external networks to enable coordination with IoT-driven remote maintenance and other services (see Fig. 4).

Conventional cybersecurity measures have used methods such as antivirus software that detects viruses using definition files, and intrusion detection systems (IDSs) that detect intrusions using signatures that express the features of known cyber-attacks. While all of these methods are effective at detecting known attacks, their inability to detect zero-day attacks is a problem.

Anomaly detection technology has become an important means of solving this problem. This technology defines normal data in advance, and detects any deviation from it as a problem. Properly defining normal data requires operations administrators who have a thorough understanding of the network configuration and all areas of the customer's business, as well as the ability to configure complex settings. However, currently, there are not enough human resources who possess these skills. Moreover, there has been a recent increase in attacks that work by skillfully misusing standard built-in commands of operating systems (OSs) or software that was not developed for attack purposes, making them difficult to distinguish from normal data.

Hitachi has responded by developing a technology that provides high-sensitivity detection of behaviors on information networks that could be misused for attack purposes, even if they are behaviors that were previously considered normal (such as the execution of standard OS commands). To allay fears that the increased sensitivity of this technology might increase the rate of false positives, Hitachi has used a cyber kill chain model* to reduce false positives by evaluating risks not only in terms of points (single phenomena), but also in terms of planes (relationships and co-occurring states among points), focusing on serial changes[3]. This technology consists of three main functions:

(1) Server/PC internal operation monitoring function

Installed on an individual server or PC for protection. Monitors events such as universal serial bus (USB) memory insertion/removal and program startup to detect suspicious behaviors.

(2) Traffic anomaly detection function

Presents a visual representation of the traffic flowing over the network, and detects suspicious communications such as by identifying whether standard OS commands could have been misused for attack purposes, or whether backdoor communication has taken place. When installing function (1) on a device is difficult, function (2) provides an effective way to monitor the device's behavior using network traffic.

(3) Evaluation function using cyber kill chain

Evaluates risks in an integrated manner using the suspicious behavior and suspicious communication detected by functions (1) and (2).

This technology can be used to detect previously undetectable skillful attacks, and solve the problem of the operations administrator shortage.

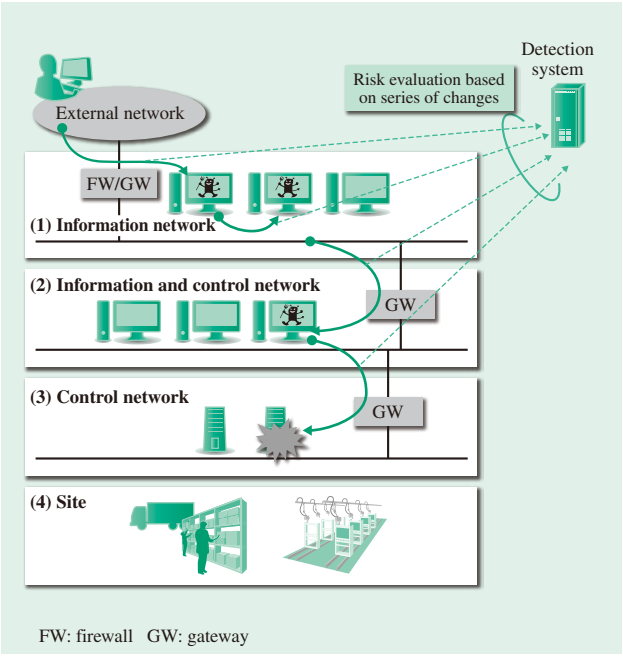

Fig. 4—IoT Value Chain Configuration.
Integrating systems from information networks through control networks, and then connecting them to external networks can improve business efficiency.

* A systematic approach to targeted attacks consisting of seven steps: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives.

CONCLUSIONS

This article has discussed the security issues that have arisen as a result of the adoption and spread of IoT systems, the approaches for solving these issues, and the detection technologies serving as the elemental technologies of these approaches.

This work was supported by the Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), "Cyber-Security for Critical Infrastructure" (funding agency: NEDO). In the future, Hitachi plans to apply the detection technologies described in this article to layered networks (information and control networks, and control networks), to carry out research and validation aimed at improving them, and then expects to put the knowledge obtained through these activities to use in new products.

REFERENCES

(1) IPA Website, "Vulnerability Countermeasure Guidelines for Control System Operators," https://www.ipa.go.jp/files/000044733.pdf in Japanese.
(2) IoT Acceleration Consortium Website, "IoT Security Trends," http://www.iotac.jp/wg/security/ in Japanese.
(3) N. Kawaguchi et al., "Detection of Advanced Persistent Threat Based on Cascade of Suspicious Activities over Multiple Internal Hosts," Transactions of Information Processing Society of Japan **57**, No. 3 (Mar. 2016) in Japanese.

ABOUT THE AUTHORS

Shinsuke Tanaka
Security Business Operation Center, IoT Business Operation, IoT & Cloud Services Business Division, Service Platform Business Division Group, Information and Communication Technology Business Division, Hitachi, Ltd. He is currently engaged in the business development of IoT security solutions.

Kenzaburo Fujishima
Network Research Department, Center for Technology Innovation – Information and Telecommunications, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of IoT systems, IoT security, and related technologies especially for critical infrastructure.

Nodoka Mimura, Dr. Eng.
Network Research Department, Center for Technology Innovation – Information and Telecommunications, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of IoT security solutions. Dr. Mimura is a member of The Institute of Electronics, Information and Communication Engineers (IEICE), the Information Processing Society of Japan (IPSJ), and IEEE.

Tetsuya Ohashi
Platform 1st Dept., IoT Development Operation, IoT & Cloud Services Business Division, Service Platform Business Division Group, Information and Communication Technology Business Division, Hitachi, Ltd. He is currently engaged in the development of network and security solutions.

Mayuko Tanaka
Security Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. She is currently engaged in the research and development of measures against cyber-attacks.