Program Director Interview

PD Interview

12 Leading Experts Who Accelerate SIP

Construct a Trustworthy Chain Connecting both Cyber and Physical Spaces

What kind of security is necessary to meet the demands of the IoT era?

With the proliferation and expansion of IoT, supply chains from various industries are connected to the Internet. The threat of cyberattacks is widely spreading to physical spaces such as manufacturing equipment connected to the Internet at plants. We interviewed program director (PD) GOTO Atsuhiro to hear how security and trustworthiness should be established to cope with both cyber and physical spaces.

GOTO Atsuhiro

President, Institute of Information Security

Response to the risks of global supply chain

Q: What are the security risks for supply chains as the IoT society develops?

PD: Let's take a look at a PC for example. It consists of different parts such as an IC chip, a camera, and a microphone, and many other parts are also supplied by various vendors to complete one product. It is not limited to hardware. Recently, highly functional software is installed in audio devices and cameras in addition to PCs and smartphones, etc. Also, a cloud service is provided by combining various IT infrastructures and services.

In this situation, if any function with malignant intent is incorporated somewhere in the supply chain, it means the products which are infected with a computer virus from the beginning will be shipped. Although PC office software can be remotely updated nowadays, it will cause serious damage if the software to be updated is infected with a virus. On the other hand, engineers apply patch files to each assembly robot individually at a plant, since centralized remote update is rather difficult. In this case, there is always a risk of contaminating the file with a virus if any operational error occurs. Avoiding such risks would be an illustrative example of robust security for the supply chain.

Many hardware parts manufacturers are connected globally. Data and software for cloud services is transmitted and shared through the Internet around the world. To address the growing risks to the global supply chain, we have been working on such challenges with two core technologies: One is for ensuring security and the other is for promptly detecting abnormalities.

Trustworthy chain in our daily life

Q: Could you tell us about the "trustworthy chain?"

PD: Assuming there is "a product infected with a virus before shipment," trustworthiness of the product would be at risk. However, our everyday life is rooted in a "trustworthy chain." "Identity verification" is a familiar example. A My Number Card and driver's license can be obtained by verifying the certificate of residence based on the family register at a city office or police station. If we present such documents for identity verification at a bank, we can open a bank account. And if we have a bank account, we can start transactions, gradually build trust, and eventually be qualified as a credit cardholder. Like "identity verification," we establish "the root of trust" first and then gradually expand that trust.

The same logic is applied to IoT devices and the supply chain. We start from "creation & confirmation of trustworthiness" as "the root of trust" and then implement "construction & distribution of a trustworthy chain." "Verification & maintenance of trustworthy chain" is also critical in ensuring safe operation. These three factors are the main themes for our R&D.

Performance and practical utility are the key to construct a trustworthy chain

Q: To reiterate your point, practical utility is also important in addition to performance for social implementation of the trustworthy chain.

PD: Security measures utilizing advanced cyber physical technology will prove their benefits only if they are available to many people. For example, the latest PC is practically embedded with a security system such as a security chip mounted next to the CPU, verifying the authenticity of the OS and ensuring safe updates. A secure chip (SCU: Secure Cryptographic Unit) we have been developing is significantly smaller in size and its power consumption is lower compared to a chip widely available on the market. Accordingly, even a micro-sized IoT device such as an embedded sensor can be "the root of trust." Also, highly tamper-resistant hardware technology automatically destroys the secure chip when it detects any suspicious activity such as extracting information, in order to ensure trustworthiness.

In addition to user-friendliness, the mechanism to ensure security is also important in the manufacturing process of the supply chain. For example, when some parts are processed by a robot arm at a manufacturing plant, the manufacturers of the robot arm are not necessarily experts in IoT security. Therefore, it is critical to provide procedure documents and manuals non-experts can easily understand and to ensure that important security features will be integrated as long as they follow the instructions to manufacture the product.

Accumulate evidence of trustworthiness across borders

Q: You have been conducting a series of demonstration experiments in the field of manufacturing, distribution, building, etc. Could you share the insight you have gained as well as the issues to be addressed?

PD: Many people are involved in a manufacturing line, a distribution, or building site and they do not necessarily work at the same location. Since they share different legal systems, safety standards, and procedures, exchanging views/ideas and reaching a consensus is essential to construct a trustworthy chain.

Recently, a building is becoming a large complex called "a smart building" or "a smart city." Electricity, water and a sewage system are provided, and elevators and escalators are controlled. They undergo frequent inspections to meet certain standards. Moreover, security guards are deployed to secure trustworthiness in terms of physical security. Currently, infection control measures have been also adopted as part of hygiene management including frequent ventilation or installation of anti-scattering acrylic plates.

Our task for demonstration experiments is to consolidate all factors and to overcome obstacles in constructing a trustworthy chain. If we take an elevator for example, the supply chain is not limited to manufacturers and operation/maintenance service vendors. As service parts which were manufactured overseas may contain personal information in the manufacturing history, we must pay close attention to the exchange of information beyond Japanese laws and regulations. We believe trustworthy evidence will be accumulated by sorting out and consolidating efforts regarding such issues.

Q: What would you like to achieve by the end of FY2022 when the second period of SIP ends?

PD: The trend of smart cities will be accelerated and IoT will make all aspects of our life even more convenient. For the immediate future, by demonstrating even a part of the ideal state of cyber physical security, we will be able to establish the foundation and expand it to smart cities and Society 5.0. Consequently, we are trying to facilitate demonstration experiments for evident trustworthy chains, such as production lines, building services, and inspection rooms for water and sewerage, etc., and showcase them as case studies.