IoT Security in a Global Environment
- For Japanese Manufacturers-

The Secure IoT Platform Consortium
President Shigeo Tsujii
March 2020

1. Overview

Despite the fast-paced, ongoing global implementation of IoT, many devices contain vulnerabilities and serious threats to cyber securities such as unauthorized manipulation by outsiders, exploitation of confidential information by phishing, data alteration, and cyberattacks which use devices as stepping stones. In cases where military or key infrastructures are targeted, huge negative impacts will be anticipated on lives.

The current state of affairs surrounding IoT can be looked at from three comprehensive viewpoints: (1) global collaboration, (2) development of international standardization and requirements for federal acquisition, and (3) global supply chain. This report will clarify the challenges for each of them and share the actions taken by the Secure IoT Platform Consortium (hereinafter referred to as SIOTP Consortium) to meet them.

2. The IoT Environment

[International Collaboration]

Since a "New Cold War" made headlines recently after Vice President Mike Pence' October 4, 2018 speech at the Hudson Institution a leading U.S. think tank. During his speech, he referred, in addition to issues related to trade barriers, intellectual property theft and illegitimate technology transfer, including military blueprints. While he discussed it in the context of national security and eventually, it led to the subsequent sanctions on Huawei.

https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-administrations-policy-toward-china/

About 30 countries and institutions including the United States, European Union, Japan, and North Atlantic Treaty Organization (NATO) attended the Prague 5G Security Conference on May 3, 2019. Adopted Chairman Statement called for participating countries to work together to avoid the risk of cyber threats, though no specific countries or entities were named . The Chairman Statement read that the IoT device life cycle needs to be managed by detecting vulnerabilities in early stages of operation, identifying and ensuring the authenticity of IoT devices and providing software patches. This likely leads to secure key management by RoT (Root of Trust) and reliable firmware updates by OTA (Over the Air).

https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf

Furthermore, prior to the G20 summit held in Osaka in June 2019, the B20 Tokyo Summit Joint Recommendations released March 2019 points out that in order to create a Society 5.0 for SDGs, it is imperative to establish a consistent and interoperable framework to manage security risks in the global supply chain.

https://www.keidanren.or.jp/policy/2019/020.html

These developments indicate we are focused on security across the global supply chain through international collaboration while monitoring the behavior of China.

[International Standards and Federal Acquisition Requirements]

Coinciding with international collaboration, international standards for identification and assurance of IoT devices over a long-life cycle are currently being developed based on the concept of zero-trust security.

●IEC 62443

This is the security standards for general-purpose control systems for industrial equipment as specified by the IEC (International Electrotechnical Commission).

Control systems in factories, plants, buildings, and power plants require security as well, but due to the closed-off nature of their operations, they have had a relatively low cybersecurity awareness, resulting in delayed implementation of security measures. The IEC 62443 sets rules for the manufacturers of control system devices, for the system integrators who use the devices to create a system, and for the user companies respectively. The SIOTP Consortium is paying close attention to the 62443-4 series in particular, which defines the security of the components that make up a system.

●NIST SP800-171

This is a set of guidelines on security countermeasures that the private sector should follow when handling controlled unclassified information (CUI) defined by the NIST (National Institute of Standards and Technology).

Companies and contractors involved in the supply chain are responsible for ensuring safety based on set security standards which cover a comprehensive range: organizations, systems, components and technologies.

The NIST SP800-171 is the security requirements for federal acquisition and is applicable to companies outside of the U.S. as long as they are in the same supply chain, i.e. U.S. allies.

●FIPS140-3

The FIPS140-3, the U.S. federal government's information security standard issued by NIST, now garners attention as a cryptographic modules standards. With respect to semiconductor devices, in order to meet strict security requirements that support the upper layer service, four levels of security requirements for semiconductors and certification tests requirements are stipulated. SSP (Sensitive Security Parameter) management, physical alteration attack resilience, non-invasive security, life cycle

management, self-testing, RoT(Root of Trust), secure boot, secure firmware updates, the complete deletion of keys and data, etc. are listed as requirements, and FIPS140-3 is expected to extend beyond the U.S. government to become the required standard for business systems around the world.

NIST SP800-140, a subseries of FIPS140-3, was finalized on March 22, 2020, and validation testing is planned to be launched on September 22, 2020.

International standards such as these lead to establishing relevant laws and regulations and are reflected in various standards for governmental acquisition. The intention of these regulations seems obvious; IoT devices that don't meet a country's security standards will be forbidden from being manufactured, to be connected to other devices, and/or to be brought into the country. We can detect the clear shift towards supply chains based on zero-trust security.

- National Defense Authorization Act for Fiscal Year 2020

The U.S. National Defense Authorization Act FY2020 was enacted on December 20, 2019 as a security requirement for defense acquisition in the United States.
https://docs.house.gov/billsthisweek/20191209/CRPT-116hrpt333.pdf

Sec. 224, in particular, defines supply chain safety requirements for microelectronics products and services to be released by January 1, 2023.

The security standards established here are expected to include international standards such as SP800-140 (the standard included in FIP140-3) with the SP800-17 at its core as the requirements for governmental acquisition.

The requirements is used as a standard for procuring products and services not only by the U.S. government agencies and consumer industries but also by U.S. allies and partner countries.

●The California State IoT Security Law

This is the first state law to define IoT device security requirements in the U.S., effective January 2020 (enacted August 2018).

It requires manufacturers of connected/connectable devices to provide an original password for each device or add a feature that urges users to change the default password.

The security requirements defined here are by no means strict but are worth noting as this is the first time IoT security legislation has come into effect.

Similar movements can be observed in Japan.

Since IoT is promoted in the global environment, similar kind of actions will be taken along with the creation of international standards in the future as well.

●Telecommunications Business Act and Technical Standard Conformity Certification

From April 1, 2020, there has been a change to the Technical Standard Conformity Certification under the Telecommunications Business Act. This modification changes the security requirements for connected/connectable devices and equipment as follows.

http://www.soumu.go.jp/main_content/000615696.pdf

Three technical standards specified in this act are: enable access control, include functionality to urge changing the default password, enable updates to the firmware. A point further worth noting is that there are recommendations for a higher level of standards concerning the identification code for access control being safely stored (RoT: Root of Trust), and firmware being safely and automatically updated (OTA: Over the Air).

[Global Supply Chain]

It is clear that COVID-19 has had a great impact not only on tourism and retail, but on the global supply chain as well. The world has realized how much it relies on China, the World's Factory, with respect to production. It was an opportunity to reevaluate the current state of affairs in the manufacturing industry.

Japan's response to the COVID-19 is a testament to our country's safety awareness, environment, and technology, and it should be a global leader in cybersecurity as well. We believe that the Japanese industry's commitment to quality and attention to details will lead to its further development, by showcasing the overwhelming safety of Japanese IoT products.

3. Approach Taken by the Secure IoT Platform Consortium

Since its establishment in April 2018, the SIOTP Consortium has been conducting research on the level of implementation of security requirements for IoT. Our motto is “Authenticity Judgement from the Individual (the device) Layer to the Cultural (the service) Layer.”

The reason we have conducted our research, despite the efforts towards the establishment and availability of international standards, is there are no guidelines for how to implement them. The results of our research were presented at the academic conferences listed below.

- Introduction of PKI Electronic Authentication for Important IoT Devices --For Establishment of Secure IoT platform--

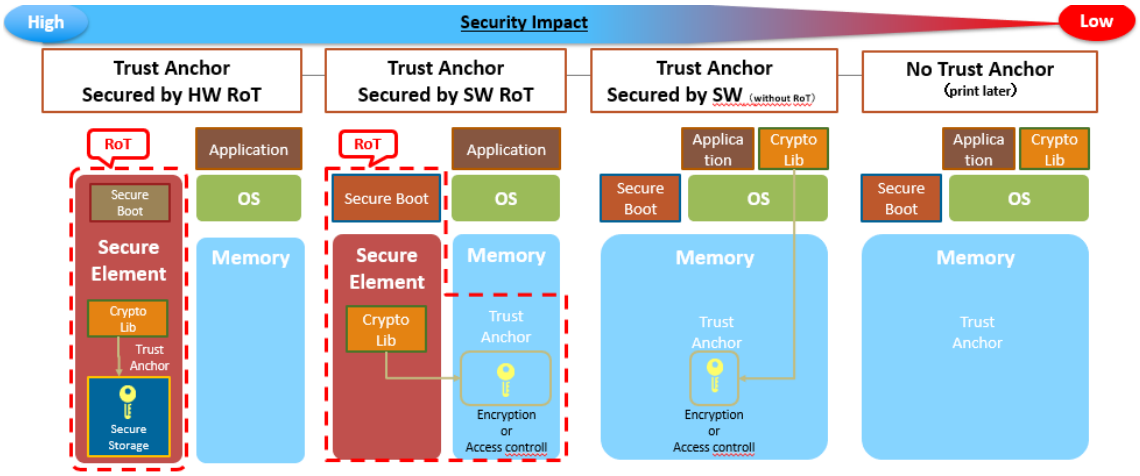
The Institute of Electronics, Information and Communication Engineers

Information Security and Electronic Communication (ISEC) 2018 (Nov. 11, 2018, Fukuoka)
- For Improvement of Genuine Level of Device, Network, Data Processing and Information Services Layers under Environment of IoT, Big Data and Artificial Intelligence
For the advancement and spread of authenticity assurance and authenticity judgment in IoT, Big Data, and the AI environment
The Institute of Electronics, Information and Communication Engineers
Cryptography and Information Security (SCIS) 2019 (Jan. 24, 2019, Kochi)
- Implementing PKI Electronic Certification on Critical IoT Devices --Trust chain formed by secure IoT infrastructure--
Information Processing Society of Japan
Information Processing: Computer Security Symposium (CSS) 2019 (Oct. 22, 2019, Nagasaki)

In these presentations, we discussed building a PKI-based trust model across the entire lifecycle.

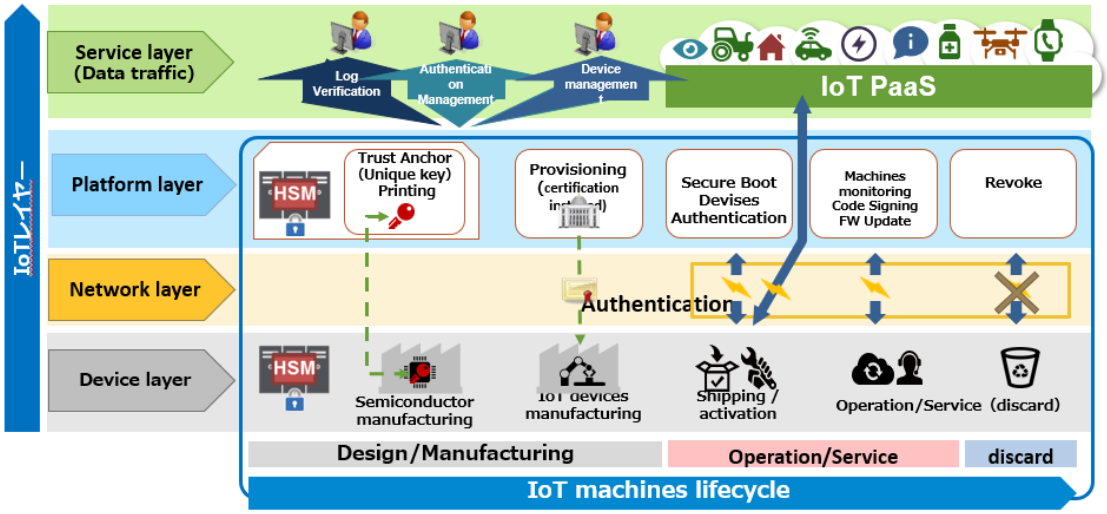
We propose to implant a universal credential in an LSI (electronic component) or so-called IC chip in IoT devices in the early stages of assembly to secure the reliability of tracing. The concept represents RoT (Root of Trust) for IoT devices. We believe Trust Anchor (original key), a credential embedded in the RoT, would be most suitable for tracing IoT devices, by using authentication structure such as PKI, where the electronic verifications have a chained structure.

●Trust Anchor and Root of Trust



These mechanisms create a trust model that realizes traceability and authenticity verification throughout the entire IoT device life cycle, from manufacturing to use to disposal (end of life).

●Life Cycle Management of IoT devices



The SIOTP Consortium will establish Standardization Subcommittee in May, where we will evaluate the effectiveness of the security implementations of our members' IoT solutions. A SIOTP Consortium Security Check Sheet has been created using our research on international standards on implementing IoT security.

3. Conclusion

In view of the current trends in the global environment, it is no longer a question as to whether or not Japan's manufacturing industry implements security, as our capacity to do business abroad is limited to our capability to implement the correct security measures.

However, the reputation for the high quality of Japanese products on the global environment will become our biggest asset, putting Japan in a position of leadership around the world. Made in Japan IoT devices will be recognized worldwide for their safety, creating a chance for immense growth, and SIOTP Consortium's task is to create specifications on implementing standards and safety evaluations to ensure the Japanese manufacturing industry capitalizes on this chance.