Charter of Trust

Partner Use Case

NXP

Principle 7 “Cyber-resilience through conformity and certification”

1. Starting point

Today, there are billions of networked IoT devices worldwide. IoT devices are used in many different areas and perform a variety of tasks. From light switches to pacemakers to critical government infrastructure such as nuclear power plants or power grids, the ability of devices across the spectrum to communicate with each other is becoming increasingly common. Forecasts predict that there will be 75 billion networked devices worldwide by 2025. This makes it possible to access all of these devices from multiple locations and retrieve data simultaneously, but it also allows cybercriminals to manipulate the devices for malicious purposes. IoT devices are highly complex with potentially large complex supply chains this gives hackers multiple points to attack. Not only could these cyberattacks be dangerous to the function of critical infrastructure, they can also be done remotely with the potential promise of huge financial gains for criminals. Additionally, they also pose a major threat to the privacy of end users. Hackers can now carry out attacks on an unprecedented scale, gathering information from private devices such as cars, smartphones, and even previously benign consumer products e.g. televisions and refrigerators, this can all happen by simply using public networks to mount their attacks.

Appropriately addressing this issue is complicated. IoT devices are complex and may consist of multiple components from different manufacturers, all of which could use different security certification standards and practices. IoT devices can have a much longer lifespan than other electronic devices such as bank cards or passports. These have a fixed lifespan and are replaced after a certain period of time, allowing manufacturers to update the security of new devices and adapt them to new attack opportunities.

IoT devices therefore need to be updated remotely to ensure they do not pose serious security risks or need to be isolated and removed from the network if compromised. In addition, there are currently no international agreed IoT certification standards for cybersecurity. Standards are the most effective tool for establishing technical regulations without imposing overly stringent requirements that may become obsolete as technology evolves or simply be too costly to achieve for an OEM operating in the cost critical IoT landscape. In the area of cybersecurity certification, achieving global standards is an important goal to ensure the safe use of IoT devices it must though be adaptable to the emerging technology and cost effective to achieve.

One example of the scale of IoT cyberattacks is Mirai, a malware that turns devices running Linux into a botnet. Mirai continuously scans the Internet for IP addresses of IoT devices and then identifies vulnerable IoT devices from a table of more than 60 common factory-preset usernames and passwords and logs into them to infect them with the malware. A Mirai malware DDoS attack that took place in October 2016 crashed several popular websites, including GitHub, Twitter, Reddit, Netflix, and Airbnb.

The impact such attacks can have on critical infrastructure is illustrated, for example, by the February 2021 attack on the Oldsmar Water Works in Florida, which attempted to raise the pH of the city's water to a dangerously high level of acidity by adding 100 times the amount of sodium hydroxide. Another example is the May 2021 attack on the Colonial pipeline, in which a leaked password allowed perpetrators to gain access to the largest fuel pipeline in the U.S. and take it out of service. Colonial paid a ransom of $4.4 million.

2. Objectives

Given the rapidly changing cybersecurity threat scenarios from malicious attackers, standardization of processes is becoming increasingly important to establish reliable security standards. With this case study, NXP aims to help lay the groundwork for the implementation of a global standard. We are confident that our work will help IoT products to be used by users worldwide with confidence in their security.

The topic of security is not adequately addressed in many companies that manufacture IoT devices. Often, the necessary expertise to implement the required security measures is also lacking, and the broad landscape of certifications does not support companies in deciding which security certification is suitable for them. A recent study by HP stated that 70 % of IoT devices "(…) contain vulnerabilities, including password security, encryption and general lack of granular user access permissions."

In order to ensure that companies implement vital security measures, it first has to be clear what the necessary security level for the product is. Standardization makes it easier for companies to identify and implement the security measures that are right for them. It promotes trust in IoT products, protects critical infrastructure and private information, which are key in the digital age.

3. Description

NXP Semiconductors is driving the implementation of the highest security standards for both its critical suppliers and its own products. Our solutions for critical applications in IoT areas such as Industry 4.0 and Industrial Automation, Connected Car, Mobile Wallets, Smart Metering, E-Government, Smart Home and Smart Cities are certified to global security standards, including Common Criteria such as ISO/IEC 15408-1...3 up to EAL 6+ level certifications, applied to the silicon, software, and critical services.

In addition, the entire NXP organization is covered by ISO27001, an international standard for information security management systems (ISMS) that includes requirements for assessing and addressing information security risks tailored to the needs of the NXP organization. NXP has also achieved certification using the Automotive ISMS standard Trusted Information Security Assessment Exchange (TISAX).

The NXP Semiconductors secure product development process and procedures are certified against the Industrial IoT standard IEC 62443-4-1 ML 2 and the newly released ISO 21434 cybersecurity standard for Automotive supply chains. Both these certifications cover the NXP development process BCaM and the Security Maturity Process (SMP) used for security products, it also covers the Product Security Incident Response Team (PSIRT) process and procedures, PSIRT details how NXP deals with cybersecurity incidents and how NXP notifies customers and stakeholders.

Our 22 major global suppliers are Common Criteria security certified and must meet stringent requirements for secure data storage, secure transactions, product security maturity and privacy protection. These certifications are conducted globally and cover the entire manufacturing process, including external wafer fabrication, mask production, wafer test rooms and semiconductor assembly. The certification bodies are located in the Netherlands, France, Spain, and Germany. Re-evaluation is due for each site after 24 months. Additionally, NXP is an active participant in the Security Evaluation Standard for IoT Platforms (SESIP) Working Group of the Global Forum. The SESIP approach to IoT security certification builds on the methodology used by Common Criteria. Based definition of a connected platform as a starting point, SESIP identifies the threat models that are most relevant to the IoT ecosystem. SESIP also includes support for certification re-use so that design elements can be repurposed without needing recertification. At NXP, we believe SESIP is critical to the growth and success of the IoT Industry as it will help build security and trust. It is practical, easy to use and reuse, and is backed by a reputable, international industry organization.

4. Lessons learned/results

The main advice we can give our customers and partners, is to make intense use of existing standards, but not to try and reinvent them single-handedly.

As a supplier of secure products for security- and safety-critical components, NXP Semiconductors has also been scrutinized by several of its customers, who initially based their assessments on self-defined requirements. Since NXP Semiconductors, as outlined above, complies to several well-known and established standards, it was never difficult to provide straightforward evidence of compliance. However, offering feedback on lengthy lists of individual compliance requirements can prove to be redundant and time-consuming, given that those are, in substance, already covered by a standard.

To address this circumstance, NXP Semiconductors pursued an open dialogue with its customers to underline the compliance portfolio already in place. In all cases, these exchanges had very positive outcomes, leading to an acceptance of our point of view, and a withdrawal of individual requirements. In some instances, individual requirements were even completely removed from the respective company's assessment processes, and replaced by international standards.