Whitepaper
2021-10

How to implement emerging IoT security guidelines

Steve Hanna, Distinguished Engineer

Abstract

Governments around the world are creating Internet of Things (IoT) security legislation and regulations designed to keep users safe in an increasingly connected world. Connectivity is good and, in fact, great but bad things can happen to people with unprotected or poorly protected IoT devices. Failing to meet these regulations or guidelines may lead to the inability to sell products in a region and thus to lost revenue. This white paper will provide background on what governments are suggesting or requiring and provide specific details on how to implement security defenses that can satisfy current and even future government requirements.

Table of contents

1 Layers for attacks in the IoT

IoT security is necessary for all the things that connect to the internet to share data. This includes smart cars, smart cities and energy, smart industry, and the smart home and its numerous consumer devices. As shown in Figure 1, the IoT architecture consists of three layers:

- Devices that send and receive data and commands
- A network that conveys data and commands
- Servers, or the cloud, that gather data, analyze and send commands

IoT devices are subject to attacks in each of these layers. On an unprotected network, an eavesdropper listening in on transmitted data or commands can reveal confidential or private information. A bad or fake server sending commands to IoT devices in the field can be used to trigger unplanned events, compromise devices, remotely load unauthorized software, cause malfunctions or even trigger a denial of service attacks, and more. A bad device injecting fake measurements can disrupt processes and cause the system to react inappropriately or dangerously. For example, security cameras are frequently attacked to spy on people or to send back normal images when a theft is actually in progress.

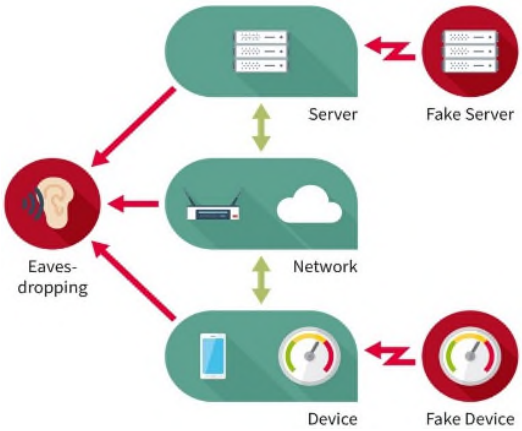

Figure 1 - Every IoT layer is a potential area for an attack.

1.1 IoT security regulations

To prevent these attacks, countries and regions around the world are creating IoT security guidelines and regulations.
In 2018, the United Kingdom's Department for Digital, Cultural, Media & Sport published its Code of Practice for Consumer IoT Security ("CoP")[1]. These 13 guidelines, listed in Table 1, identify good practices for IoT security. The UK is now considering making their current recommendations mandatory.
Table 1. The 13 Guidelines in the UK Code of Practice for Consumer IoT Security[1].

1. No default passwords
2. Implement a vulnerability disclosure policy
3. Keep software updated
4. Securely store credentials and security-sensitive data
5. Communicate securely
6. Minimize exposed attack surfaces
7. Ensure software integrity
8. Ensure that personal data is protected
9. Make systems resilient to outages
10. Monitor telemetry data

11. Make it easy for consumers to delete personal data
12. Make installation and maintenance of devices easy
13. Validate input data

At this point, the CoP is perhaps the best-established and most targeted guidelines. In 2019, the guidelines were adopted as an international standard: ETSI TS 103 645. The European Union (EU) has announced that it will adopt these guidelines and make them mandatory. Mandatory regulations usually include penalties and, in this case, could eventually prevent the sale of products within the regulating region. Singapore also adopted the UK regulations and will initially make them voluntary. As attacks and problems mount, more countries will likely adopt these guidelines and make them mandatory.
In May 2020, the U.S. National Institute of Standards and Technology (NIST) released information report (IR) NISTIR 8259A[2], IoT Device Cybersecurity Capability Core Baseline. This document provides cybersecurity best practices and guidance for IoT device manufacturers. Table 2 shows the six capabilities recommended by this document.

1. Unique logical and physical IDs
2. Only authorized entities can change device configuration
3. Protect stored and transmitted data from unauthorized access and mods
4. Restrict access to local and network interfaces, protocols, and services
5. Permit software and firmware updates using secure, configurable mechanism
6. Report device cybersecurity state to authorized parties

Table 2. Device cybersecurity recommendations identified in NISTIR 8259A.

In December 2020, the IoT Cybersecurity Improvement Act of 2020[3], previously approved by both Houses of Congress by unanimous consent, was signed into law by the President. This unprecedented unity to address a national security problem in these contentious times confirms its importance and the confidence in the solution.

The provisions contained in this bill direct NIST to develop guidelines for security of IoT devices purchased by the U.S. government. It also directs the Office of Management and Budget to develop rules for agencies to follow when they purchase IoT devices in the future.
While the NIST Guidelines are still in development, they are available for review in draft form in NISTIR 8359D (Draft). Going further than NISTIR 8359A to strengthen cyber security for government applications, manufacturers should be aware of and interested in the future changes and prepare for their implementation.

Two other U.S. cyber security requirements were implemented by the executive branch in response to major attacks.

Developed in response to the SolarWinds cybersecurity attack (discovered Dec 13, 2020), the Executive Order on Improving the Nation's Cybersecurity[4], May 12, 2021 was announced to improve the software and services used by the Federal Government. This order requires several changes regarding how service providers for US Government operate. Changes include: (1) prompt reporting of security incidences by service providers; (2) required compliance of service providers to best practices for secure software development; (3) requirements for government agencies to implement multifactor authentication

and other established security procedures; and (4) requires NIST to initiate a pilot program for IoT security device labeling for consumers.

After the Colonial Pipeline Cyber Attack (April 2021), steps were taken to protect critical and vulnerable infrastructure in the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems[5], July 28, 2021. This document describes the approach the executive branch is taking to improve cyber security in critical infrastructure. Under the umbrella of a voluntary, collaborative effort between the Federal government and the critical infrastructure community, sector- specific guidance is being developed for IoT cyber security for critical infrastructure.

Other legislation in the U.S. is occurring at the state level. California became the first state to pass an Internet of Things cybersecurity law. Effective on January 1, 2020, California state law SB-327[6] that was passed in 2017, requires manufacturers of any device connected to the internet (IoT-device) that want to sell their products in California to include "appropriate" security feature(s). Manufacturers failing to do so will face enforcement from the California Attorney General and local officials. “Smart” devices that connect “directly or indirectly” to the internet, must be equipped with security measures to prevent unauthorized access, destruction, use, modification, or disclosure. Manufacturers have a safe harbor if the device either:

- Includes a unique preprogrammed password for remote access OR
- Requires users to generate a new authentication means before the first access

Authentication is highlighted in this law because it is so fundamental to IoT security. With weak authentication like a default password, attackers can easily log into a device and control it. Well-designed IoT devices use strong measures such as hardware security to prevent such attacks.
In addition, effective January 1, 2020, an Oregon state law (OR HB-2395)[7], enacted in 2019, requires manufacturers of IoT devices sold in Oregon to include “reasonable security features … appropriate to the nature and function of the device.” Violations constitute an “unlawful trade practice” under existing Oregon law, which means a violation prevents the sale of products in Oregon.
Even if these laws are at the state level today, manufacturers are unlikely to create different versions of their products for those that ship only to California or Oregon, so the net result is that manufacturers have to introduce device security in all their products.

This growing trend of IoT security regulations seems unlikely to abate soon.

1.1.1 IoT defenses

Different security defenses are required in many facets of the IoT to avoid weaknesses for exploitation to satisfy security requirements. Figure 2 identifies 10 areas, many of which are outlined in the UK CoP and other regulations. However, without the help of security experts, it is not realistic to expect IoT device manufacturers to know the right defenses to employ. Device manufacturers are experts, and even world leaders, in building equipment such as washing machines, cars, and other products. However, the required depth of knowledge in networked device security is not often readily available in their organizations

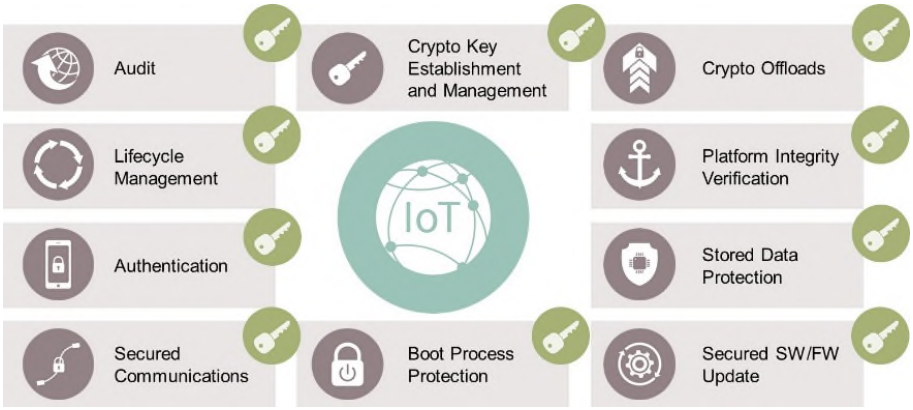

Figure 2 – A broad range of defenses exist to protect IoT devices.

Security hardware makes it easier for product manufacturers to design and produce secure IoT devices and makes it easier for users to install and use these devices. Infineon offers a wide range of security hardware products, allowing the customer to choose the product that best meets the needs of their application. Figure 3 shows the range of security processors/products in Infineon's AIROC™, Programmable System-On-Chip™ (PSoC™), OPTIGA™ Trust and OPTIGA™ TPM solutions.

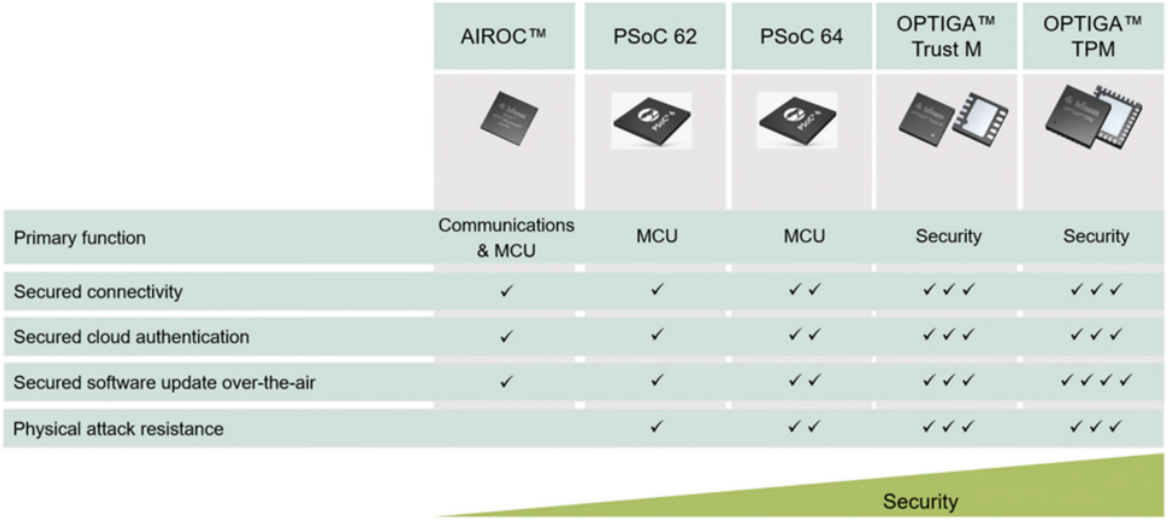

Figure 3 – Infineon's hardware-based security products span a range of capabilities.

.

1.1.1.1 How to meet the toughest regulations

A careful look at the UK Code of Practice (CoP) and NISTIR 8259A shows that many of these requirements are best met with hardware security. The choice of hardware over software-based security will not change with new legislation and regulations. For example, items 1 and 4 in the CoP (Table 1) and item 1 in the NISTIR 8259A list (Table 2) indicate the need for strong authentication with well-protected credentials.

Fortunately, the OPTIGA™ solutions include a unique cryptographic key pair and certificate stored in hardware – the highest and strongest kind of authentication available. By integrating an OPTIGA™ solution into an IoT device, device manufacturers can quickly and easily meet these government

requirements and probably any future ones relating to IoT device identity. Beyond this, the OPTIGA™ family of security solutions can be used for strong authentication of users, servers, etc.
Items 4, 5, and 8 in the CoP match with item 3 in NISTIR 8259A, requiring secured communications and storage. The best place to store sensitive data is in a security chip, as supported by the OPTIGA™ solutions.

Large data items and secured communications are typically protected with bulk encryption implemented on the main processor for maximum throughput. Even in those cases, OPTIGA™ products can play several essential roles. First, generating an encryption key requires high-quality entropy (cryptographic randomness) which the OPTIGA™ solutions are designed to provide. Second, secured communications are meaningless without strong authentication to prevent attackers from posing a man-in-the-middle (MitM) attack. Third, secured storage requires a place to store the encryption key or key-encryption key, as supported by the OPTIGA™ solutions.

Item 3 in the CoP and item 5 in NISTIR 8259A require support for updating software on IoT devices. Installing security updates is as important for IoT devices as it is for phones and computers. To prevent the installation of malicious updates, the signature of each update needs to be checked. The best way to do this is by using a verification key stored in hardware, like an OPTIGA™ solution.

Checking software integrity (item 7 in CoP) is typically performed during the boot sequence. As the device boots up, it uses a key (preferably stored in hardware such as an OPTIGA™ solutions) and checks the signature on all of its software to make sure it is OK before running it.

There are a variety of ways to accomplish Item 9, “make systems resilient to outages.” One way is by having everything residing local to the system, so if the internet goes out, the device still works. This requires the device to be secured and not require the cloud for its security. The built-in hardware-based security performs this task.

If the internet is available, the best way to “monitor telemetry data,” Item 10, is through remote attestation, which is best accomplished with the OPTIGA™ security solutions to prevent malware from subverting the process. With remote attestation, the cloud can monitor the device to verify it is running the latest and proper software. The fundamentals of this feature are implemented in the OPTIGA™ TPM with additional software that resides in the cloud. The TPM makes measurements during the boot sequence and reports these measurements later to the cloud as telemetry data to verify that the device has not been attacked or tampered with.

The best way to “make it easy for consumers to delete personal data,” Item 11, is to encrypt personal data with a key and store that key in the security chip. When the consumer no longer needs to access the information, because of a sale or even end of life of the device, deleting the key eliminates the possibility of using it to decrypt the personal encrypted data. Unlike erasing software, which can allow a determined attacker to retrieve and restore data, the destruction of an encryption key instantly renders the encrypted data completely meaningless.

Item 12 (“easy installation and maintenance”) sounds simple. Unfortunately, making it easy for the consumer to securely install an IoT device is quite difficult. The OPTIGA™ family of security solutions are designed to integrate quickly and securely with all the major IoT clouds such as Microsoft Azure, Amazon AWS, Google Cloud and more. The device manufacturer gets a security chip that is ready for easy cloud integration.

Item 13 (“validate input data”) is always good advice. However, it has proven devilishly difficult for IoT devices. Daily news reports show that even thoroughly vetted software can be vulnerable to malicious packets that may cause a buffer to overwrite and compromise the device thus giving it access to all data and keys accessible to the main processor. For this reason, long-term keys and critical secrets should not be accessible to the main processor. OPTIGA™ solutions are the best place for such secrets.

.

Security for today and the future

After years of attackers exploiting IoT device weaknesses, governments around the world are finally starting to take preventive action. With its intent “to ensure that products are secure by design,” the UK Code of Practice[1] provides excellent guidelines for what is needed to provide security in today’s IoT devices. Thus, it is not surprising that these rules are being adopted in the European Union’s and Singapore’s regulations. Similar requirements are found in USA guidelines such as NISTIR 8259A. As demonstrated by NISTIR 8259D and recent executive orders, one may reasonably expect these rules to tighten over time as more security is needed. To avoid premature product obsolescence, device manufacturers should adopt strong security solutions like the AIROC™, PSoC™ and OPTIGA™ solutions that can be used to meet the increasingly stringent requirements for IoT security emerging from governments all around the world.

Doing the best job possible for designing an IoT product starts with hardware-based security to provide best-in-class security and preparation for the most rigorous security requirements --- both today and in the future.

References

[1] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

[2] https://www.nist.gov/news-events/news/2020/06/security-iot-device-manufacturers-nist-publishes-nistirs-8259-and-8259a

[3] National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems: https://csrc.nist.gov/publications/detail/nistir/8259d/draft

[4] Executive order on improving the nation's cybersecurity, and Security Memorandum on improving cybersecurity for critical infrastructure control systems: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[5] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

[6] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327

[7] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327

Published by
Infineon Technologies AG
85579 Neubiberg, Germany

Date: 2021-10