How to build trust in your Internet of Medical Things (IoMT) device using PSA Certified components, paired with Secure Boot and Vulnerability Management

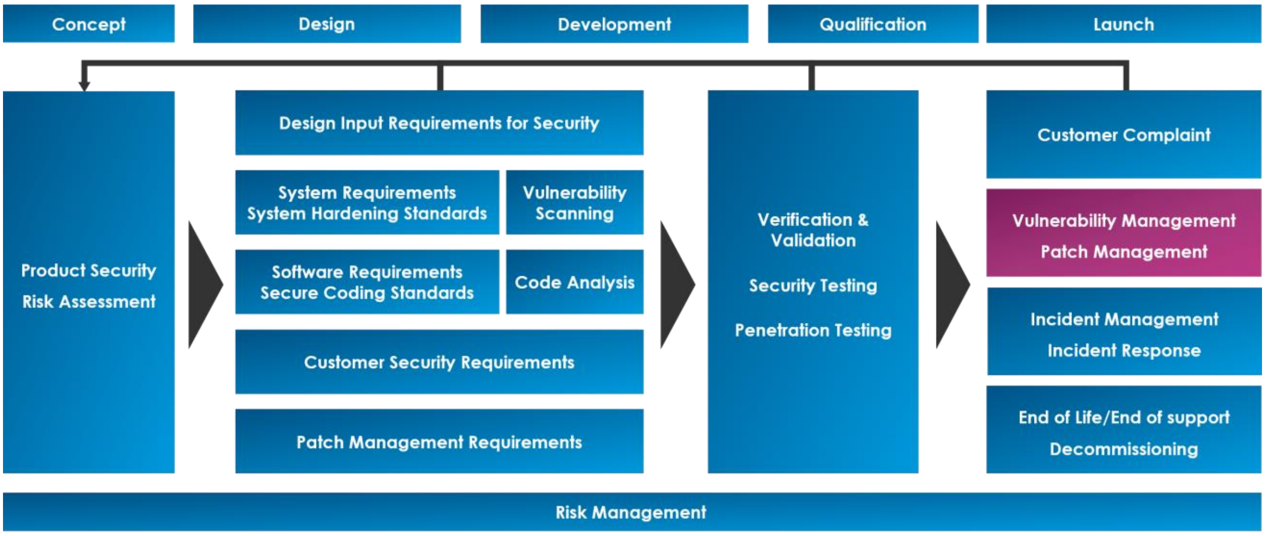
When we think about the security of IoT products, we usually focus on protecting information confidentiality, integrity, and availability. In a healthcare setting, we have an additional and weightier responsibility, to keep people safe.

We must:

- protect sensitive patient information from being disclosed should a data breach occur,
- mitigate the risk of a denial-of-service attack, which could prevent someone from using a device, depleting the product's battery, or preventing data from being sent to the clinician, and
- ensure only genuine software is used on a device, to avoid incorrect diagnosis or treatment.

However, the implications are not limited to patient harm, there are also a number of business risks such as reputation damage, discontinuity of service and revenue loss for anyone involved in the development of the device. This is why it is important to Flex to ensure our products are being built on a strong foundation of security, that is, Root of Trust, such as the PSA-RoT outlined by PSA Certified.

At Flex we have integrated cybersecurity best practices in our Product Development Life Cycle following the suggestions proposed in the "Medical Device and Health IT Joint Security Plan" available here.

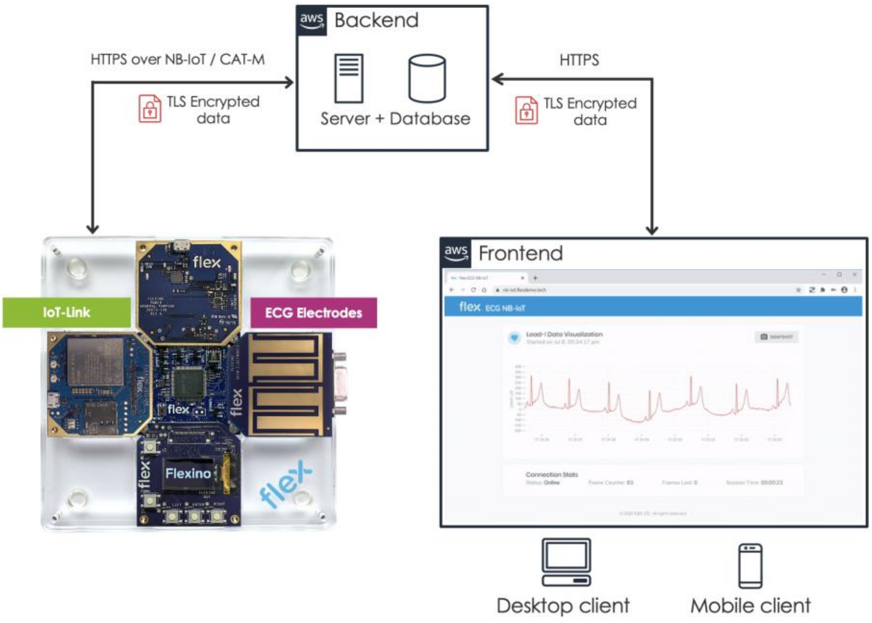

Concept
Design
Development
Qualification
Launch
Product Security Risk Assessment
Design Input Requirements for Security
System Requirements System Hardening Standards
Vulnerability Scanning
Software Requirements Secure Coding Standards
Code Analysis
Customer Security Requirements
Patch Management Requirements
Verification & Validation
Security Testing
Penetration Testing
Customer Complaint
Vulnerability Management Patch Management
Incident Management Incident Response
End of Life/End of support Decommissioning
Risk Management

Product Security Framework: It shows how the product commercialization phases (top row) relate to the product security activities (core row). Source: "Medical Device and Health IT Joint Security Plan".

This paper offers insights on our Vulnerability Management process using our PSA Certified Level 1 Sensor Integration Platform, Flexino, as reference. It also illustrates how using an ecosystem of certified system software and silicon chips can help navigate the complexity of designing security into a device.

Flex Sensor Integration Platform

Our modular platform enables customers to streamline development while maintaining security. It offers more than 40 hardware and software building blocks that can be ported into any product architecture with minimal intervention. For this use case, we used our medical-grade analog front-end to acquire the patient's ECG signal and send it over NB-IoT to a server. This enabled a practitioner to visualize the ECG trace in real time using the web application you see in the picture below.



Communication Architecture for our Remote Patient Monitoring reference application.

We carefully selected pre-verified hardware architecture which is based on the [PSA Certified Level 1 STM32L4 from STMicroelectronics (based on the Arm Cortex-M4)](). While hardware development is complete, there are frequent software updates, making use of the [PSA Certified Level 1 FreeRTOS]() system software. On top of selecting pre-certified components, Flex is proud that the Flexino Sensor Integration Platform is PSA Certified Level 1, reflecting a proactive investment in security and adherence to security best practice.

> The PSA Certified status we were awarded assures our customers that their products are being built on a strong foundation of security, that is, a Root of Trust, and they will be compliant with the major standards and regulations driving cybersecurity for connected devices - NIST 8259A and ETSI EN 303 645.

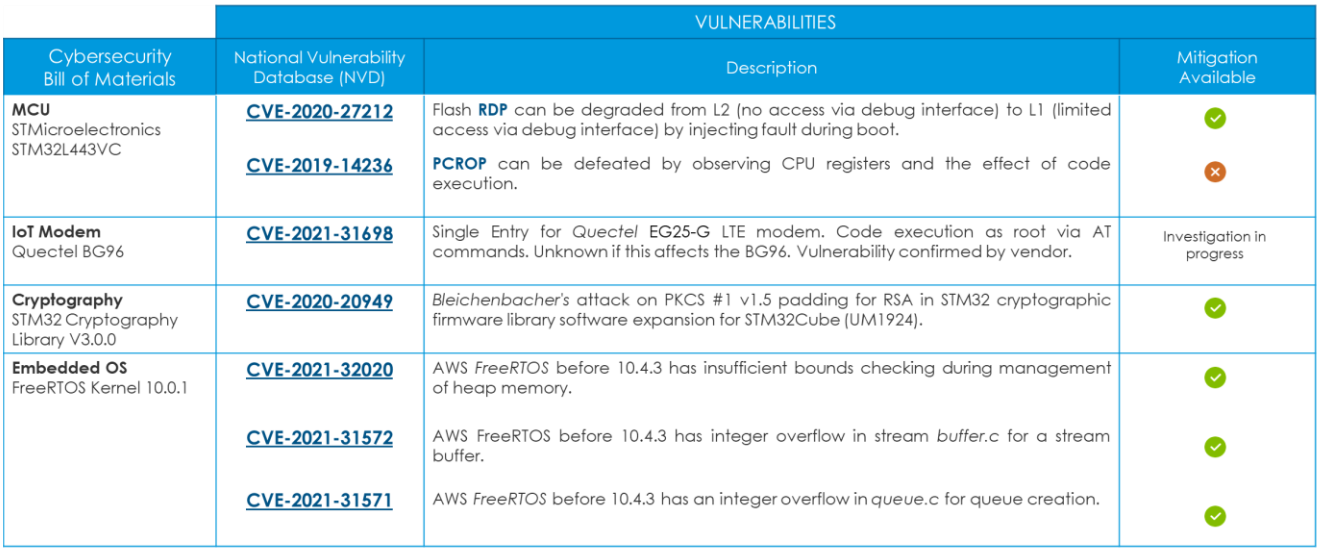
Juan Cols,
Innovation Engineer, Sensors & Actuators Centre of Excellence, Flex

Cybersecurity BOM

Since the hardware is based on off-the-shelf components, we need to keep track of possible risk exposures. A bill of materials (BOM) is a comprehensive list of parts, components and subassemblies required to manufacture a product. We can extend the same concept to software and so create a Cybersecurity BOM (CBOM). This is the first step towards continuously monitoring new vulnerabilities that might compromise the security of your device and allows remedial action to be taken if that's the case.

Vulnerability Monitoring Example

In the table below you can see a simplified version of the CBOM for our reference platform. We listed the microcontroller, the IoT modem, some cryptography libraries and real-time operating system. We also listed some of the vulnerabilities reported for each component in the National Vulnerability Database from the NIST (National Institute of Standards and Technology) which you can access here.



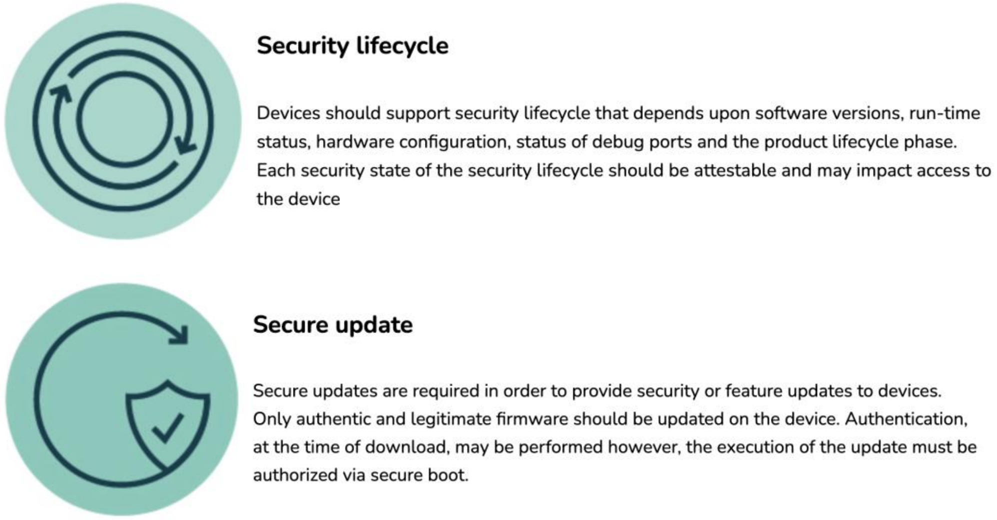
Cybersecurity Bill of Materials	VULNERABILITIES		
	National Vulnerability Database (NVD)	Description	Mitigation Available
MCU STMicroelectronics STM32L443VC	CVE-2020-27212	Flash **RDP** can be degraded from L2 (no access via debug interface) to L1 (limited access via debug interface) by injecting fault during boot.	✓
	CVE-2019-14236	**PCROP** can be defeated by observing CPU registers and the effect of code execution.	✗
IoT Modem Quectel BG96	CVE-2021-31698	Single Entry for *Quectel* EG25-G LTE modem. Code execution as root via AT commands. Unknown if this affects the BG96. Vulnerability confirmed by vendor.	Investigation in progress
Cryptography STM32 Cryptography Library V3.0.0	CVE-2020-20949	*Bleichenbacher's* attack on PKCS #1 v1.5 padding for RSA in STM32 cryptographic firmware library software expansion for STM32Cube (UM1924).	✓
Embedded OS FreeRTOS Kernel 10.0.1	CVE-2021-32020	AWS *FreeRTOS* before 10.4.3 has insufficient bounds checking during management of heap memory.	✓
	CVE-2021-31572	AWS FreeRTOS before 10.4.3 has integer overflow in stream *buffer.c* for a stream buffer.	✓
	CVE-2021-31571	AWS *FreeRTOS* before 10.4.3 has an integer overflow in *queue.c* for queue creation.	✓

Cybersecurity Bill of Materials (CBOM) for Flex's Sensor Integration Platform.

The risk assessment of the new vulnerabilities is necessary to understand the risk for the system/user. For example, the first entry in the table (CVE-2020-27212) affects the Root of Trust of the device.

Taking Action

The PSA Certified 10 Security Goals outline best practice ways to combat the most common threats to connected devices. Achieving the Security Lifecycle goal, paired with Secure Update helps to patch new vulnerabilities when they are highlighted in the CBOM.



Security lifecycle

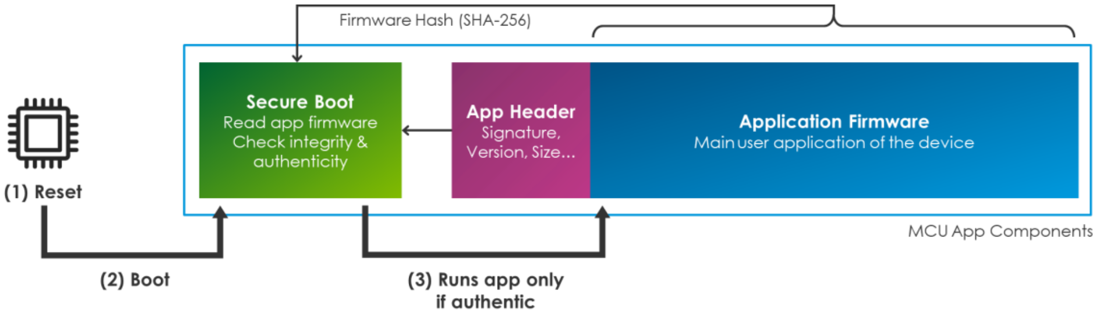
Devices should support security lifecycle that depends upon software versions, run-time status, hardware configuration, status of debug ports and the product lifecycle phase. Each security state of the security lifecycle should be attestable and may impact access to the device

Secure update

Secure updates are required in order to provide security or feature updates to devices. Only authentic and legitimate firmware should be updated on the device. Authentication, at the time of download, may be performed however, the execution of the update must be authorized via secure boot.

Two of the PSA Certified Security Goals outlined in this whitepaper.

Let's see the process we followed to achieve the Secure Update Goal by releasing a new firmware (FW) update to maintain the Root of Trust of our platform.


Firmware Hash (SHA-256)
Secure Boot
Read app firmware
Check integrity & authenticity
App Header
Signature, Version, Size...
Application Firmware
Main user application of the device
(1) Reset
MCU App Components
(2) Boot
(3) Runs app only if authentic

The different app components in a typical embedded Chain of Trust.

In this diagram you can see the different app components that form our firmware: The Secure Boot which is responsible for checking the integrity and authenticity of the User Application. The User Application itself, which implements the acquisition of the ECG signal and its transmission to the backend server. And the App Header, which contains some metadata as the Digital Signature of the User App, version and its size in number of bytes. In a Chain of Trust each different app component is responsible for the security of the other and the anchor at the beginning of this chain is our Root of Trust, implemented here by the Secure Boot.

We can talk about **Root of Trust** only if this app component fulfills two key properties:

1. **Single entry point**. Meaning that every time the hardware resets this is the first piece of code that runs.
2. **Immutable**. In other words, once the Secure Boot has been downloaded onto the device memory, it cannot be changed.

By exploiting the CVE-2020-27212 vulnerability reported before, an attacker can disable the hardware protections that assure the Root of Trust of the device. This was demonstrated by researchers from the Fraunhofer Institute of Applied and Integrated Technology. In their paper they also proposed effective countermeasures to mitigate this vulnerability, which we followed and implemented in a new FW update. If you are interested in the details of the analysis, attack, and countermeasure, you can find them here.

As the market continues to grow and IoMT products become mainstream, hackers' interest in the sector will grow alongside it. Our role in the industry is to build trust in innovative connected devices, to secure acceptance of new technologies. Emerging regulations and baseline requirements are changing the way we see security, ensuring that the benefits of remote healthcare devices do not come at the expense of patients' privacy or safety.

Further Reading

- Access the PSA Certified certificate for Flex's Sensor Integration Platform
- Learn more about the Flexino Sensor Integration Platform on flex.com
- Flex Talk on 'Cybersecurity for Connected Medical Devices'
- Learn more about IoT Security for the Remote Healthcare Market
- PSA Certified 10 Security Goals

If you'd like to speak to someone at Flex, please e-mail: **healthsolutions@flex.com**