Surviving the IoT Wave

EMSPARK™ SECURITY SUITE

www.sequiturlabs.com
TABLE OF CONTENTS

IoT SECURITY—NOT OPTIONAL ANYMORE..............................................................3
SEQUITUR EmSPARK™ SECURITY SUITE.............................................................3
EmSPARK™’s CAPABILITIES.....................................................................................4
Secure the Boot Chain..........................................................................................4
Isolate Security Critical Resources......................................................................4
Protect Critical IP...................................................................................................4
Manage Keys and Certificates................................................................................5
Update Device Firmware Securely.........................................................................5
Enable Security Throughout the Supply Chain....................................................5
Build Resilient Products.........................................................................................5
Prevent Device Class Breaks..................................................................................5
GETTING STARTED WITH THE EmSPARK™ SECURITY SUITE..........................5
Supported Processor Platforms............................................................................5
EmSPARK™ SECURITY SUITE COMPONENTS......................................................6
CoreTEE™ Trusted Execution Environment.........................................................6
CoreLockr-TZ™......................................................................................................6
Tools.......................................................................................................................6
Software Development Kit (SDK) The EmSPARK™ SDK.....................................6
Free Evaluation Kits.............................................................................................6
Partner Development Platforms..........................................................................7
REAL WORLD EXAMPLES—EmSPARK™-BASED SOLUTIONS..........................7
Building Management Systems (featuring Johnson Controls)............................7
Home Security Systems (featuring Boundary Technologies, Ltd.)........................7
Machine Vision – Critical Intellectual Property (AI/ML Code) Protection)...........8
Biometric Readers...............................................................................................8
LET’S SUMMARIZE..............................................................................................9
WHAT DO I DO NEXT?.........................................................................................9
IoT SECURITY—
NOT OPTIONAL ANYMORE

S
decurity is on everyone’s mind these days. As a device maker, you want to focus on building your device and the application. Your customers, however, now want to be assured that your device is safe to operate on their network. You understand that without a proper security framework, your brand, your revenues and reputation are all at risk. It does not matter whether you are building a control system, medical device, a biometric reader, a wearable or an industrial gateway—device security is simply not optional anymore.

SEQUITUR EmSPARK™ SECURITY SUITE

Developing a secure IoT product requires addressing security issues that arise throughout a device’s lifecycle. That covers a wide range of features and functions:

+ Verifying that the device is using verified and safe firmware when it boots and updates.
+ Protecting the critical IP that you’ve developed to make your solution the best in your industry, including machine learning or artificial intelligence code.
+ Detecting, reporting and recovering from a security threat.
+ Protecting the device from physical and remote attacks, from being the target of attacks to becoming part of a botnet that attacks other devices and networks.
+ Ensuring that these best-in-class security features are implemented and upgraded safely and correctly throughout the supply chain.
+ Securely integrating your fleet of IoT devices with a cloud application

This is a large undertaking for any developer. It requires a deep understanding of security, cryptography, memory architecture, silicon, operating systems and application design. Confronted by this new challenge IoT device vendors still need deliver great products on time, using the resources they currently have. It is not easy. Even if you dedicate substantial resources for security, it is still not easy.

Solving this problem is the mission of Sequitur Labs and the EmSPARK™ Security Suite. EmSPARK™ was created to provide a general-purpose security framework for ANY kind of connected device for a variety markets, including:

+ Industrial Automation
+ Machine Vision
+ Smart Home
+ Building Automation
+ Medical Devices
+ Biometric Readers
+ Smart Cities
+ Building Management Systems
+ Energy and Smart Grid

Security is on everyone’s mind these days. As a device maker, you want to focus on building your device and the application. Your customers, however, now want to be assured that your device is safe to operate on their network. You understand that without a proper security framework, your brand, your revenues and reputation are all at risk. It does not matter whether you are building a control system, medical device, a biometric reader, a wearable or an industrial gateway—device security is simply not optional anymore.

SEQUITUR EmSPARK™ SECURITY SUITE

Developing a secure IoT product requires addressing security issues that arise throughout a device’s lifecycle. That covers a wide range of features and functions:

+ Verifying that the device is using verified and safe firmware when it boots and updates.
+ Protecting the critical IP that you’ve developed to make your solution the best in your industry, including machine learning or artificial intelligence code.
+ Detecting, reporting and recovering from a security threat.
+ Protecting the device from physical and remote attacks, from being the target of attacks to becoming part of a botnet that attacks other devices and networks.
+ Ensuring that these best-in-class security features are implemented and upgraded safely and correctly throughout the supply chain.
+ Securely integrating your fleet of IoT devices with a cloud application

This is a large undertaking for any developer. It requires a deep understanding of security, cryptography, memory architecture, silicon, operating systems and application design. Confronted by this new challenge IoT device vendors still need deliver great products on time, using the resources they currently have. It is not easy. Even if you dedicate substantial resources for security, it is still not easy.

Solving this problem is the mission of Sequitur Labs and the EmSPARK™ Security Suite. EmSPARK™ was created to provide a general-purpose security framework for ANY kind of connected device for a variety markets, including:

+ Industrial Automation
+ Machine Vision
+ Smart Home
+ Building Automation
+ Medical Devices
+ Biometric Readers
+ Smart Cities
+ Building Management Systems
+ Energy and Smart Grid
EmSPARK™’s CAPABILITIES

With the EmSPARK™ platform you can:

+ **Secure the Boot Chain:** Building secure devices begins with a trusted boot chain. This goes beyond a simple firmware check at boot time; it means securing the boot process from initial ROM boot all the way to deployment of a trusted, authenticated copy of your Operating System (ex. Linux), and your firmware. EmSPARK™ implements a unique encrypted boot chain that extends secure boot capabilities of the hardware platform. This process ensures the fidelity of your firmware, preventing theft or compromise by malware. The process also results in a device ID which is tied to the hardware root of trust (RoT), making it immutable and hence trustworthy.

+ **Isolate Security Critical Resources:** The principal of isolation is fundamental to creating secure devices. Sensitive material such as encryption and decryption keys should be isolated from the application itself to limit the impact of an attack. Isolation is achieved via a system partition by reserving certain memory addresses as secure and others as non-secure. Referred to as a “Secure Enclave,” it functions as an integrated security co-processor capable of executing instructions that are independent of, and shielded from, a rich operating system (OS) such as Linux. It also includes a Trusted Execution Environment (TEE), which is essentially a secure OS that runs concurrently with the rich OS. On Arm®-based processors, an on-chip secure enclave is established using Arm® TrustZone® technology, and Sequitur’s CoreTEE™ Trusted Execution Environment. CoreTEE™ is currently the only commercial TEE optimized for embedded and IoT devices. EmSPARK™ provides a complete solution for security isolation—setting up the secure enclave as part of the boot process.

+ **Protect Critical IP, including Machine Learning and Artificial Intelligence algorithms:** ML/Al algorithms are the most important asset of many IoT device vendors, and protecting them from theft or corruption is critical. EmSPARK™ ensures the security of these algorithms by housing the applications in the Secure Enclave and only allowing access to them through the Trusted Execution Environment (TEE). For application development, EmSPARK™ security suites are pre-configured to fully enable the hardware security features available on your microprocessor. For example, EmSPARK™ makes it easy to make use of hardware crypto accelerators with support for symmetric and asymmetric encryption schemes. The platform includes CoreLockr™—a small footprint middleware layer that includes robust APIs, allowing easy to access security features and greatly reducing the learning curve for developing secure applications.

*Creating a secure, trustworthy product requires taking deliberate steps to implement specific security technologies to enable the right kind of protection.*

—Phil Attfield, CEO

---

**FIGURE 1:** Hardware Isolation (TrustZone) is provided by the processor. The Sequitur Labs CoreTEE™ Trusted Execution Environment implements the Secure Enclave.

+ Memory partitioning
+ Isolation of critical security resources
+ Protection for critical IP and algorithms
+ Software integrity enforced by secure hardware
EmSPARK™ provides Trusted Applications (TA) for cryptography, secure storage, and certificate management. For further application development, APIs available in the platform include:

+ Cryptography
+ Certificate Management
+ Secure Storage
+ Open SSL
+ Secure Payload Verification

A Linux distribution optimized for use on the processor is also included.

**+ Manage Keys and Certificates:** Throughout its lifecycle, an embedded or IoT device uses different keys and certificates. Keys and certificates are used for many operations such as boot, secure firmware update and for secure TLS based connections to IoT cloud platforms. EmSPARK™ includes robust key and certificate management tools to achieve a variety of security goals.

Certificate management is a critical part of the trust chain. Managing certificates is only allowed via commands signed with a device vendor’s private key. This reduces the threat of malicious software attempting to breach the certificate repository. Certificate management functions include loading, deleting, updating, revoking and verifying certificates.

**Figure 2:** Use of Keys and Certificates in IoT

**+ Update Device Firmware Securely:**
Updating a device’s firmware and applications securely is a critical requirement and one where risk of firmware compromise is high. Incoming firmware payloads need to be authenticated to prevent corruption and compromise. EmSPARK™ provides key and certificate based payload authentication mechanisms to ensure secure updates.

**+ Enable Security Throughout the Supply Chain:** Firmware theft at time of device manufacture, storage and shipping is a rampant problem leading to unauthorized cloning of devices and loss of revenue. EmSPARK™ gives you the tools to inject multiple keys and certificates securely, ensuring authenticated and protected firmware throughout the product delivery process. Advanced key management features allow for change of ownership and role delegation.

**+ Build Resilient Products:** Resilient devices embody “self-healing” capabilities thereby reducing the need to service and/or physically replace them. EmSPARK™ supports advanced features such as real-time integrity checking to monitor integrity of the Linux kernel and providing graceful remediation in case of kernel compromise.

**+ Prevent Device Class Breaks:** Many device makers implement a single root key, typically stored in the device ROM, across all devices of a particular type. A class break occurs when this key is compromised leaving every device using that key exposed. EmSPARK™ provides the framework for each device to have a unique key tied to its hardware root of trust. This makes it an immutable ID and can therefore be trusted in various security related processes.

**Getting Started with the EmSPARK™ Security Suite**

**Supported Processor Platforms**

EmSPARK™ Security Suite are are supported
on industry-leading IoT processors. EmSPARK™’s capabilities are pre-configured for each supported product. The primary differences between the products relate to integration with hardware crypto engines and the secure boot process. OEMs and developers are not impacted since EmSPARK™ abstracts the underlying complexity. Currently EmSPARK™ supports the following microprocessors:

+ NXP i.MX6
+ NXP i.MX7
+ NXP i.MX8
+ Microchip SAMA5D7

EmSPARK™ supports the hardware security components available simplifying the task of developing secure products.

**EmSPARK™ SECURITY SUITE COMPONENTS**

The EmSPARK™ Security Suite has the following components:

**CoreTEE™ Trusted Execution Environment**

The CoreTEE™ Trusted Execution Environment creates the foundation for your secure device architecture. It houses a secure operating system which executes secure boot, update and recovery, creates the Secure Enclave and executes Sequitur’s Trusted Applications (Crypto, Secure Storage and Key/Certificate Management). The CoreTEE™ also allows you to develop your own Trusted Applications (TAs). Finally, the CoreTEE™ provides an easy way to access device peripherals. For example, payment terminal developers may need to secure the LCD display to protect against malware (such as key stroke loggers designed capture passwords and other credentials). Securing the LCD requires integrating the LCD driver into a Trusted Execution Environment so that the use of the display only occurs when the device is in a secure state. You can read more [here](#).

**CoreLockr-TZ™**

CoreLockr-TZ™ is a security framework for microcontrollers that takes advantage of Arm’s TrustZone for V8M architecture. It allows designating a set of memory addresses as secure and provides Sequitur’s API’s (Cryptography, Certificate Management, Storage, Open SSL and Payload Verification), for developers to make use of secure processes. Read more [here](#).

**Tools**

The EmSPARK™ suite provides code examples, linux patches for enabling CoreTEE™, a firmware packing tool, OpenSSL Crypto Engine, and a toolchain and client API for easy implementation of the software.

**Software Development Kit (SDK) The EmSPARK™ SDK**

Software Development Kit (SDK) The EmSPARK™ SDK is a tool enabling developers to built their own Trusted Applications (ex. AI/ML Algorithms) for integration into the EmSPARK™ secure environment.

**Free Evaluation Kits**

Evaluation kits supporting our partners’ processor platforms are available here:

**EmSPARK™ for NXP**

**EmSPARK™ for Microchip**

The evaluation kits provide evaluation code, application examples and documentation.
Partner Development Platforms

EmSPARK™ is supported on the following partner development platforms:

ARROW SHIELD96 TRUSTED PLATFORM

The Shield96 Trusted Platform comes preloaded with the EmSPARK™ Security Suite software by Sequitur Labs. This provides a secure platform applicable across all IoT verticals to enable secure end point solutions and protect firmware, keys and data throughout the lifecycle of a product. EmSPARK™ is the essential software companion suite complementing the Microchip hardware providing a cost-effective secure solution appropriate for every connected device built with the ATSAMA5D2 processor. Engineers can leverage this reference design for digital transformation built on trust extracting the full value of the advanced embedded security features of the ATSAMA5D2. More details are available here.

MICROCHIP ATSAMA5D27-SOM1

The SAM5D2-SOM1 is a small single-sided System-On-Module (SOM) based on the high-performance 32-bit Arm® Cortex®-A5 processor-based MPU SAM5D27 running up to 500 MHz. The SAM5D27 SOM1 is built on a common set of proven Microchip components to reduce time to market by simplifying hardware design and software development. The SOM also simplifies design rules of the main application board, reducing overall PCB complexity and cost. The SAM5D27-SOM1 is delivered with a free Linux distribution and bare metal C code examples.

MICROCHIP ATSAMA5D2C-XULT

The SAM5D2 Xplained Ultra is a fast prototyping and evaluation platform for the SAM5D2 series of microprocessors (MPUs). The board includes eMMC and DDR3 memories as well as a rich set of connectivity options. Connectors and expansion headers allows for easy customization and quick access to leading edge embedded features such as the Class D amplifier or the capacitive touch controller (PTC). A Linux distribution and software package allows you to easily get started with your development.

REAL WORLD EXAMPLES—EmSPARK™-BASED SOLUTIONS

EmSPARK™ is a general-purpose security framework for securing a broad range of embedded devices. We highlight a few below:

Building Management Systems (featuring Johnson Controls)

The Johnson Controls Metasys Building Automation System creates intelligent environments by connecting HVAC, lighting, security and protection systems on a single platform to deliver the information building operators need to help ensure comfort, safety and security for building occupants. Johnson Controls required a solution with a high assurance of product security, spanning the development, manufacturing, and entire life cycle of their products. Read the full case study here.

Home Security Systems (featuring Boundary Technologies, Ltd.)

Boundary Technologies, Ltd. offers a smart intruder alarm, built to UK & European standards, which can be remotely monitored with a smartphone. The product can be adapted to suit individual needs, from the number of sensors required to installation options. Boundary required a solution that included best-in-class data and software protection for its product. This included key and certificate management, secure over-the-air (OTA) firmware updates and secure payload verification for assuring the integrity of critical home safety functions. Read the full case study here.

An industry-leading vendor of machine vision products required a solution to protect its Artificial Intelligence and Machine Learning (AI/ML) algorithms used to support its technology. Machine Vision products follow the process of 1) acquiring an image of a product or process, 2) processing the data delivered by the image, and 3) making critical decisions (such as quality or acceptance of a product or process) based on the data. The algorithms that deliver this functionality represent critical intellectual property (IP), and create significant value for the products. It is absolutely business critical that these algorithms are protected, and can only be seen and used by developers of the products themselves.

Read the Case Study here.

Biometric Readers

Biometric identification is fast becoming a global reality. Take India’s Aadhar Card scheme for example, which is considered as the single largest biometric capture and use project in the world. The scheme calls for capturing biometric data (finger print and iris scans) for nearly a billion citizens. Further, communication accounts (mobile numbers), financial and banking accounts (Know Your Customer data) are all linked to the above biometrics. Major transations such as home buying or financial investment activity can only occur with biometric verification of participants. Such a system must pay particular attention to the security of the system including the risk of biometric devices being hacked or otherwise compromised.

FIGURE 3: Biometric Reader with EmSPARK™ Security Suite for SAMA5D2

Source: Sequitur Labs and Tech Rizes
Let’s Summarize

Getting security right for embedded and IoT devices is a critical but daunting task. The fragmentation of platforms, the complexity of hardware security and time to market pressures have all contributed to a need for a complete IoT security solution. EmSPARK™ delivers the framework flexible enough to address diverse security needs, simplifying the task of building secure, trustworthy devices.

WHAT DO I DO NEXT?

Evaluate EmSPARK™ for yourself. Go to www.sequiturlabs.com and get a FREE software evaluation kit and try it! If you have a specific problem you are trying to solve, drop us an email at info@sequiturlabs.com.