Surviving the IoT Wave

SEQUITUR LABS SECURITY PLATFORM

www.sequiturlabs.com

SEQUITUR LABS

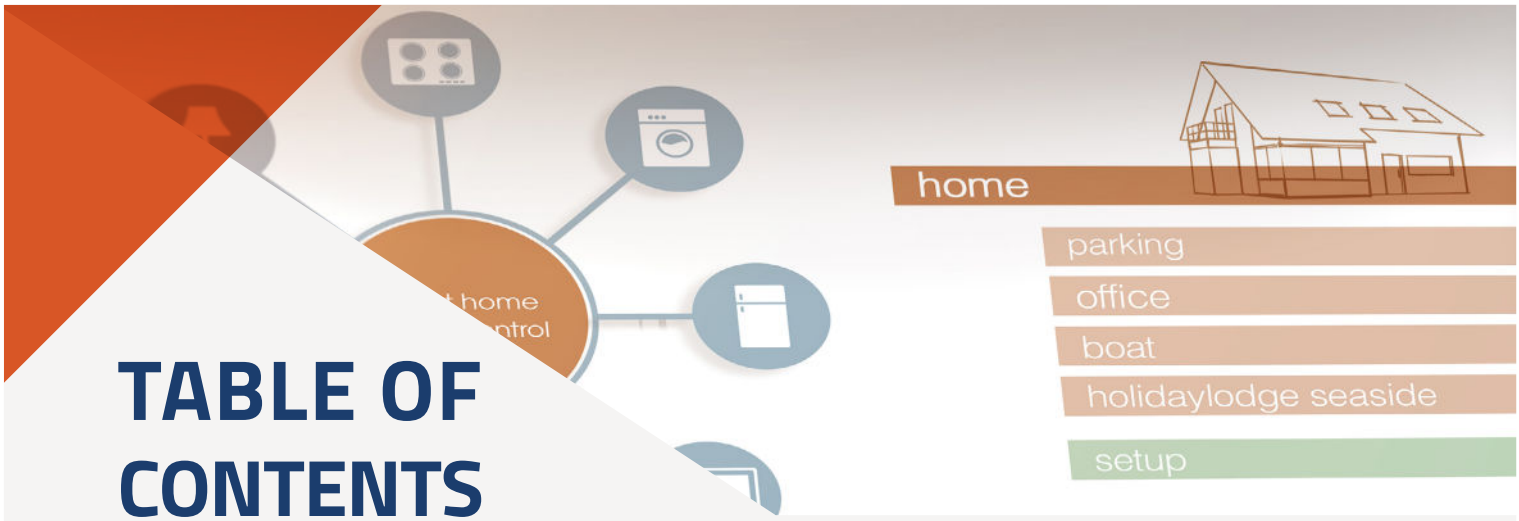


TABLE OF CONTENTS

IoT SECURITY— NOT OPTIONAL ANYMORE

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 LABS SECURITY PLATFORM

Developing, deploying and managing 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 code or artificial intelligence models.
+ 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.

With the exciting acceleration of the deployment of AI Models at the network edge, this problem only becomes more complex—and the need for solutions more urgent.

Solving this problem is the mission of Sequitur Labs and the Sequitur Labs Security Platform. The platform 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**
+ **Smart Cities**
+ **Building Management Systems**
+ **Energy and Smart Grid**

The Sequitur Labs Security Platform has two products:

+ **EmSPARK™ Security Suite:** A software package consisting of firmware, integration tools, and APIs that provides complete chip-to-cloud security for MPU's.

+ **EmPOWER™ Cloud Services:** A SaaS solution providing the services needed to secure, provision, update and manage intelligent edge devices.

CAPABILITIES

With the Sequitur Labs Security 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/AI 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, pre-built applications are available to fully enable the hardware security features 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

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.

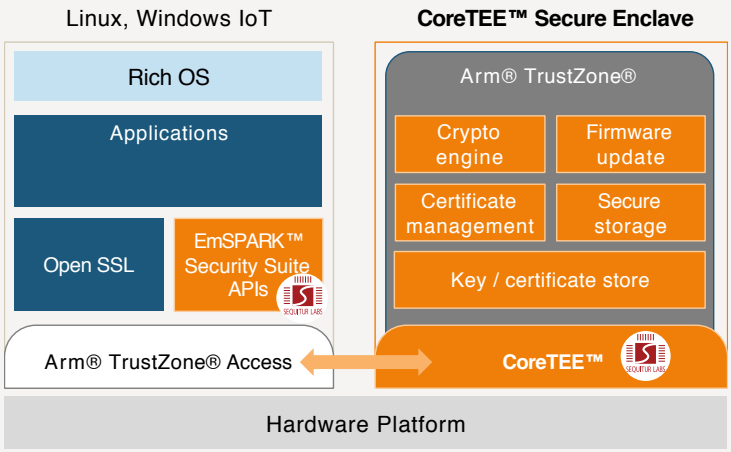


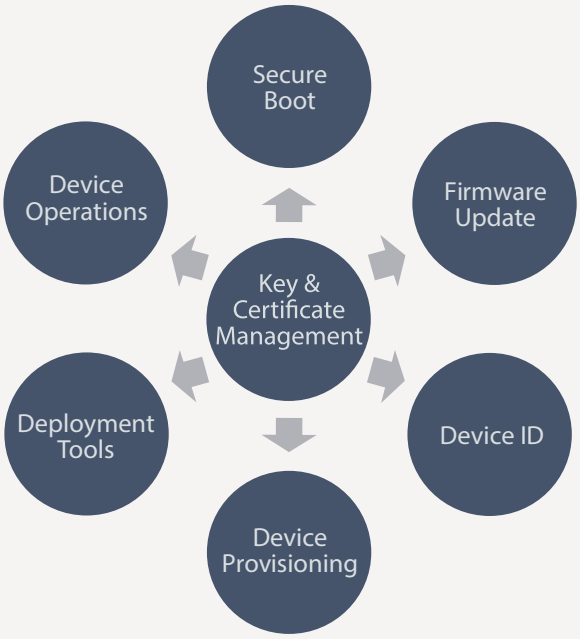
FIGURE 1: *Hardware Isolation (TrustZone) is provided by the processor. The Sequitur Labs CoreTEE™ Trusted Execution Environment implements the Secure Enclave.*

- *Memory partitioning*
- *Isolation of critical security resources*
- *Protection for critical IP and algorithms*
- *Software integrity enforced by secure hardware*

- **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™ and EmPOWER™ provide 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 deliver 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.

+ **Integrate Securely with Cloud Platforms:** Device integration with cloud platforms, such as AWS IoT Core or Microsoft Azure IoT, creates a variety of exciting opportunities for any IoT application. Cloud platforms enable management and monitoring of devices at a large scale. Integration with purpose-built analytics applications that can be used to optimize the performance of a fleet of devices, becomes practical. Additionally, today's applications processors can deliver a rich array of data regarding the health and security state of an IoT device. This data can be used to identify and address threats. With pre-built applications for easy cloud integration and mutual authentication and control, developers can reliably integrate these features.

EmSPARK™ SECURITY SUITE

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. You can 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)

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

EmPOWER™ CLOUD SERVICES

EmPOWER™ is a SaaS solution that provides the essential cloud services needed to secure, provision, update and manage intelligent edge devices. OEM's can manage and update products securely, detect and respond to threats, protect against intellectual property theft, and gain secure insights into a fleet of thousands of devices. EmPOWER™ is seamlessly integrated with the EmSPARK™ Security suite, with additional support for MCU's with secure elements. EmPOWER's key services, which complete the chip-to-cloud security solution, include:

Mutual Authentication for Command and Control

In order to maintain a trusted relationship between the device and the cloud, the two entities must establish a mutually authentication connection. This results in authtenticated, trusted command and control, which affects all elements of device management in the cloud: registration, updates, threat detection, monitoring, etc.

Secure Over-the-Air Updates

Most processes for device updates are not secure because 1) the connection and commands are not mutually authenticated and 2) update tools and services are not housed in the TrustZone secure enclave. But ensuring these two elements, EmPOWER™ maintains a trusted, relable update process between the device and the cloud.

Threat Detection and Remediation

Today's microprocessors can detect and transmit a wide array of information about a device, including anomalies, tampers, and other threats. In order for this information to be useful and actionable, the data must be trusted, authenticated and sometimes encrypted. With EmPOWER™'s mutually authenticated connection with EmSPARK™ enabled devices, this trusted information can be used to detect threats and take appropriate actions to protect a device.

REAL WORLD EXAMPLES—SEQUITUR LABS SECURITY PLATFORM 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.

Machine Vision – Critical Intellectual Property (AI/ML Code) Protection

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 full case study here.

GETTING STARTED WITH THE SEQUITUR LABS SECURITY PLATFORM

Supported Processor & SOM Platforms

EmSPARK™ Security Suite 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 platforms from Microchip, NVIDIA, NXP and STMicroelectronics. ArrowShield96 Trusted Development Board, and Variscite i.MX 8 SOM family provide support for EmSPARK™ out of the box. EmSPARK™ supports the hardware security components available simplifying the task of developing secure products.

Evaluation Kits and Subscriptions

To get started with EmSPARK™, choose the free evaluation kit for your microprocessor. To check out EmPOWER™, contact us at info@sequiturlabs.com for a trial subscription.

Learn More

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

EmSPARK™ for Microchip

EmSPARK™ for NXP

EmSPARK™ for NVIDIA

EmSPARK™ for STMicroelectronics

EmSPARK™ for Arrow Shield96

EmSPARK™ for Variscite

The evaluation kits provide evaluation code, application examples and documentation.

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.

SEQUITUR LABS

Sequitur Labs is developing technologies for the development and management of secure and trustworthy connected devices. Sequitur's products span a range of disciplines required for trusted computing, from boot through the full device lifecycle. Sequitur's security solutions provide real business value to device makers, such as reducing BoM costs, protecting revenue by thwarting IP theft, improving product reliability and reducing liability, and improving device lifecycle management processes. To learn more about Sequitur's security platform, visit us at www.sequiturlabs.com.

Sequitur Labs Inc.,
PO Box 1127
Issaquah, WA 98027

+1 425 654 2048
+44 20 3318 1171

info@sequiturlabs.com
www.sequiturlabs.com

©2021 Sequitur Labs Inc. All rights reserved.

TrustZone is a registered trademark of ARM Limited (or its subsidiaries) in the US and/or elsewhere.

MWPEm-0001 Rev B. Printed in the U.S.A.