Secure Software Provisioning—IP Theft Prevention with EmSPARK™ Security Suite

Firmware theft at time of device manufacture, storage, or shipping, is a rampant problem that leads to unauthorized cloning of devices and loss of revenue. For many IoT device manufactures, firmware IP represents much of the value of a company's product or brand, and simply cannot be compromised.

Threat mitigation in the product fulfillment process are summarized below.

IP THEFT. This can be controlled by a minimal installation process, in which the IP is never accessed by manufacturers. All images are encrypted and the device will only be able to run provisioning when the device has been configured to boot securely. Additionally, the provisioning application must verify the device processor, or System-on-Chip (SoC), authenticity and ensure that it is running securely, prior to starting the provisioning process.

OVERPRODUCTION OR COUNTERFEITING. To prevent overproduction, each device is authorized to install the firmware late in the installation process. This controls the number of firmware images. Alternatively, the following controls can be put in place:

- Control the number of devices that allow provisioning of real firmware at the factory
- Forced connection to a remote server to authorize each firmware installation
- Connect to a local device, which limits the number of installations

PROTECT THE ROOT OF TRUST (RoT) PROVISIONED KEYS. Random keys for the RoT and unique device identification are generated during provisioning. Provisioning payloads are re-keyed. (This should be done on secured device.) Private keys are never to be extracted from a device.

EmSPARK™ provides the tools to secure firmware during product fulfillment. Multiple keys and certificates are injected securely, ensuring authenticated and protected firmware throughout the product delivery process. Advanced key management features allow for change of ownership and role delegation. The secure software provisioning process is outlined below.

HARDWARE VALIDATION: Typically, initial hardware validation is performed prior to provisioning any secure payloads.

PRE-PROVISIONING:

- At the beginning of this stage, flash memory is clear, and the processor (SoC) is untouched.
- A bootloader, or external tool, is configured to boot securely.

PROVISIONING PROCESS BEGINS:

1. The system now reboots with the provisioning application.
2. The provisioning application performs the following tasks:
   - Decrypts payloads
   - Generates a device key
   - Generates a device certificate signing request
   - Encrypts the payloads using a freshly generated diversified key
   - Replaces the provisioning bootloader with the production bootloader
3. Fuses are now set on the SoC.

TRANSITION TO PRODUCTION:

- Flash now contains the production bootloader, EmSPARK™'s CoreTEE™, and supporting files such as Linux file systems and U-Boot.
- The secure boot process is initialized to authenticate and install the production applications. For more details, see the Secure Boot Solutions Brief.

Learn More

EVAL KIT

Download the free evaluation kits and user's guide for more details and code examples

Download "Surviving The IoT Wave: EmSPARK™ Security Suite" Whitepaper

A **FREE** EmSPARK™ Security Suite Evaluation Kit is available at: https://www.sequiturlabs.com/iot-security-suite/free-iss-eval-kit.

SEQUITUR LABS

Sequitur Labs is developing seminal technologies to improve trust in a connected world, reducing the cost and complexity to build secure embedded and IoT 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.

PO Box 1127
Issaquah, WA 98027

+1 425 654 2048
+44 20 3318 1171

info@sequiturlabs.com
www.sequiturlabs.com

MSBEm-0004-Rev A. Printed in the U.S.A.