Secure Firmware Updates with the EmSPARK™ Security Suite

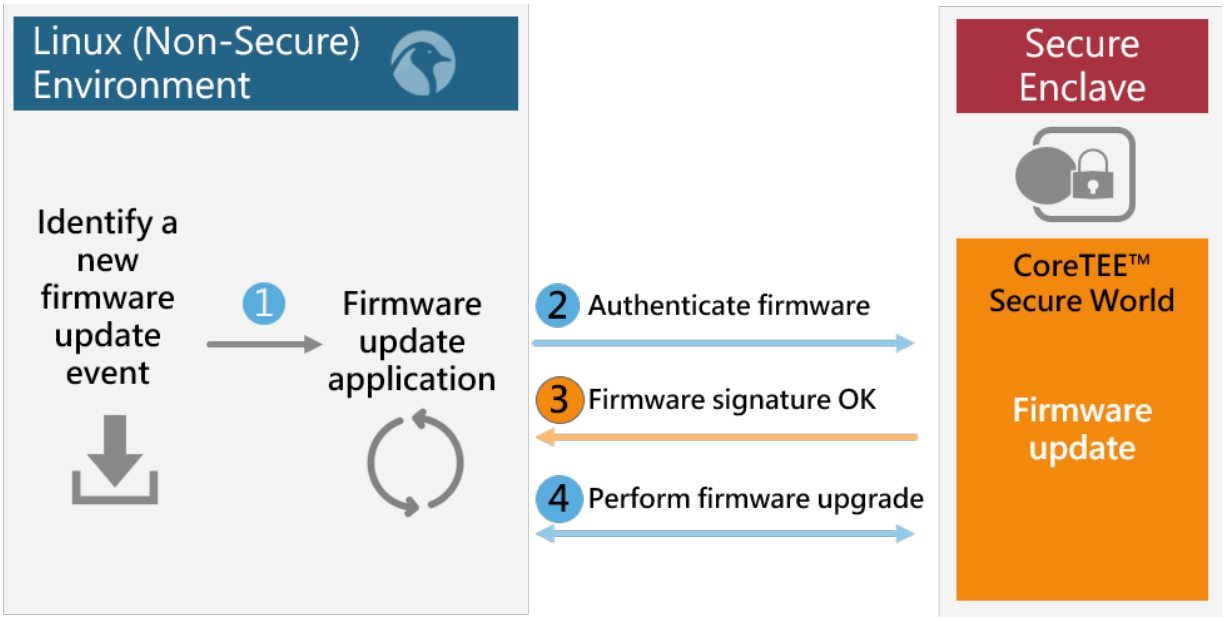
An IoT device must be maintained to remain useful. To ensure that the device is running at peak performance throughout its lifecycle, firmware updates, administered locally via a network, or Over-the-Air (OTA), are essential. It is during the update process when the device is most vulnerable to compromise, and a secure process is critical.

Secure firmware updates are intricately tied to the Secure Boot. (It is recommended to review Secure Boot Solutions Brief prior to this solutions brief.) For updates, the steps are as follows:

1. A device application manages a schedule or set of events that determine that an update will be performed.
2. When prompted for an update, the device performs a re-boot, with boot state variables signaling that the device will follow an update process prior to the secure boot process.
3. The Read-Only Memory (ROM) then loads and verifies the Secondary Boot Loader (SPL).
4. The device determines—by memory and registers holding the boot state variable and reset status—that the boot process is an update.
5. The device locates and reads the payload in the update location.
6. The update software is loaded, and the update's Binary Large Object (BLOB) payload is verified by checking its signature.
7. An update key is generated to de-crypt the payloads.
8. The update is re-encrypted with the device's diversified key (see Secure Boot Solutions Brief), and stored to the specified location.
9. The device then attempts to perform a Secure Boot process as normal with the freshly applied update.
10. Following the Secure Boot process, the shared memory and Sequitur CoreTEE™ is established, and Rich Environment functions, such as UBoot and Linux kernels, are loaded.

EmSPARK™ also provides a payload verification API for validating application updates. This API can also be used by Linux to validate an update package prior to initiating the update process. This allows for validating the integrity of the update package prior to initiating the reboot.

The payload validation process is shown below:



The EmSPARK™ Security Suite automates this process by providing:

1. Key and certificate-based payload authentication
2. Coordination with Rich OS (e.g., Linux) encryption file system
3. Locations for storing update payloads
4. Signing and encryption of a new firmware image

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

SEQUITUR LABS

PO Box 1127
Issaquah, WA 98027

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 or follow us at @SequiturLabs.

MSBEm-0002-Rev A. Printed in the U.S.A.