Securing Your Embedded System Life Cycle

Introduction Paper

Introduction

To protect an embedded system from the growing threats of financial loss from network-based attacks or board-level tampering, it is critical to secure a design throughout the entire life cycle—from device fabrication, to system decommissioning. It is convenient to separate the component supply chain life cycle from the embedded system life cycle. This paper builds on the material in the "Securing Your Supply Chain Life Cycle" paper, listed in the "To Learn More" section at the end of this paper; to cover the complete life cycle of your embedded system.

Any embedded system undergoes several stages in its life cycle, as illustrated in Figure 1 below. This article will describe each of the main lifecycle phases—Design/Development, Manufacturing, Deployment, Field Upgrade, and Decommission, and will introduce appropriate security measures that can be used in each phase.

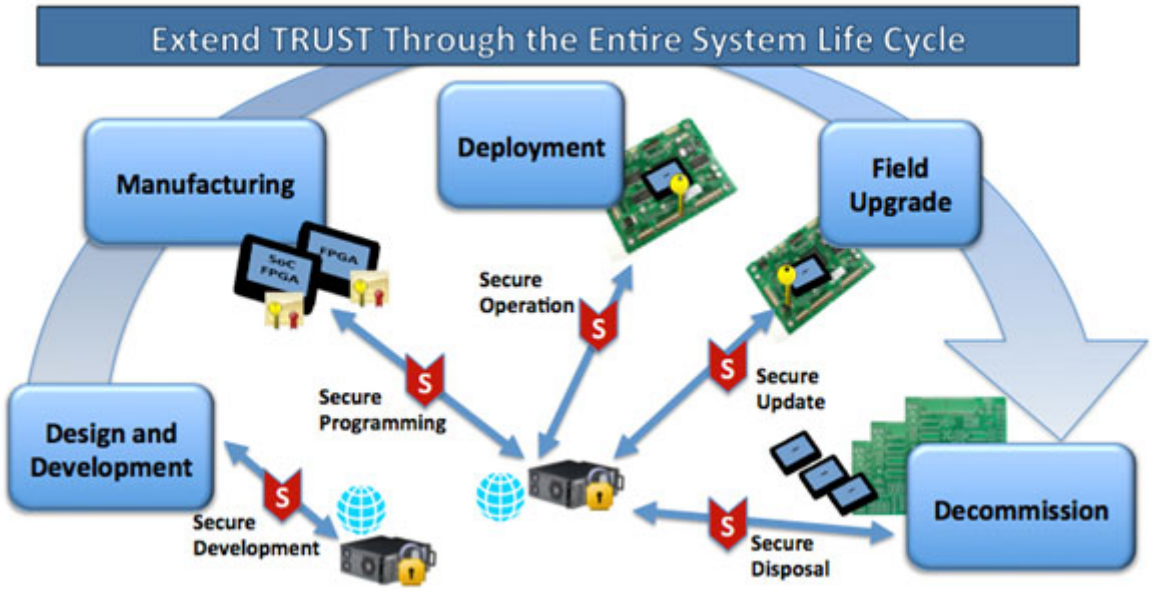

Figure 1: **Implementing a Secure Embedded Life Cycle**

Requirements for Securing the Embedded System for the Entire Life Cycle

The design and development of the embedded system is typically the most trusted stage of the process. The embedded system company can control the design process and should do this as a part of a standard development procedure.

However, manufacturing, deployment, field upgrades, and decommissioning are typically done outside of the direct ‘control’ of the OEM, and have specific security requirements that must be followed to create a secure lifecycle. Additionally, a secure device needs to be used as the starting point for any secure embedded system lifecycle. If this device doesn’t have a secure supply chain it can’t be the Root-of-Trust (RoT) of a secure lifecycle. A RoT is the secure source for secret keys and cryptographic services on which all other security capabilities rely.

We will assume that a device with a secure supply chain, like the IGLOO®2 or SmartFusion®2 SoC FPGAs from Microsemi, are used as the RoT in the embedded system. These devices use inherently secure on-chip non-volatile configuration memory, support a host of features for secure key storage, and provide advanced real-time cryptographic services that implement unique and secure device identification— creating the most secure supply chain available.

For more details on the techniques used to secure the entire device supply chain refer to the material listed in the "To Learn More" section at the end of this paper.

Electronics Manufacturing

During manufacturing it is critical to insure that the RoT device is programmed securely. The use of an encrypted bitstream can help improve security, but only if the associated secret keys are loaded securely and not in a ‘plain-text’ form. Encrypting key loading allows devices to be safely handled in a less-trusted factory environment since they are protected by encryption. This prevents several types of malicious attacks such as eavesdropping, impersonating a device, bitstream substitution or modification, and overbuilding.

It is also useful for secure devices to include a Certificate of Conformance (CoC), which includes the device serial number along with keyed digests for each bitstream component that was programmed. This ensures that the CoC tags from each device are different, even if the programmed data is the same. The programmer tool can validate the returned CoC messages from each device, and report this in secure log files for tight accounting control over the number and identity of parts produced or scrapped.

IGLOO2 and SmartFusion2 devices support truly secure loading of the user bitstream keys in encrypted form, and include comprehensive CoC capabilities. Microsemi also offers productized hardware, software, and tools to assist the user in building a production infrastructure for secure management of their bitstream keys. For more details on the techniques used to secure your design during manufacturing refer to the material listed in the "To Learn More" section at the end of this paper.

System Deployment

During deployment the embedded system is the most vulnerable to malicious attacks and tampering. The system must be protected from remote network based attacks as well as physical probes of critical signals and attempts to identify security keys using side-channel attacks. Differential Power Analysis (DPA) is an advanced side-channel attack that can determine secret keys through a statistical analysis of power changes during security operations. The use of DPA countermeasures, like those used in the billions of deployed smartcards and set-top boxes, can dramatically improve key security.

Network-based attacks can be particularly malicious because the equipment being controlled by the embedded system can be hijacked, or even permanently compromised. Implementing a secure boot process; where the RoT device contains the immutable boot loader and verifies the authenticity of the various code elements used in the multi-stage boot process, as shown in Figure 2 on page 3, is just one key element in securing an embedded system from a network attack.

You can learn more about the Secure Boot process in "Overview of Secure Boot with Microsemi SmartFusion2 SoC FPGAs".

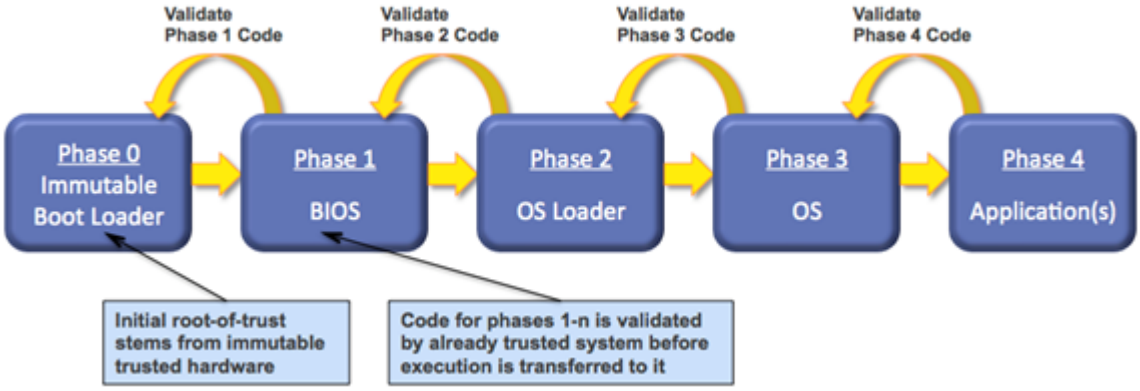

Figure 2: **Secure Boot Process Diagram**

Physical attacks to FPGAs are also a threat and FPGAs that store configuration data externally are particularly threatened, since they require a data transfer on each reset and can be subject to repeated observation. On-chip flash-based configuration memory, that directly controls the routing switches and look-up tables of the FPGA fabric, greatly enhances security by eliminating the observation of configuration data during reset.

IGLOO2 and SmartFusion2 devices incorporate DPA countermeasures to protect security keys, implement RoT for secure boot processes, and use on-chip non-volatile memory to further protect on-chip data. Many other security related features like: zeroization, device passcodes, segmented key management, no data read-back option, NVM integrity check, and hardware firewalls enhance device security to the highest possible level. For more details on the techniques used to secure your design once it is deployed in the field, refer to the material listed in the "To Learn More" section at the end of this paper.

System Field Upgrades

In many cases it is desirable to upgrade an embedded system with new firmware—either for the FPGA or the MCU. Using secure key storage and encrypted bitstreams support secure remote programming and bitstream files that are fully authenticated, also provide proof of integrity and heritage. If the security device implements an In-Application Programming (IAP) Service, so no other controlling device is involved, system security is further enhanced.

Care must be taken so that the upgrade process doesn't provide a malicious attacker with an avenue of attack. For example, if an older version of an image can be used to update a device, adversaries could re-introduce a more vulnerable firmware version. It is important to include back-level version control so that known vulnerable images can't be re-introduced.

Microsemi IGLOO2 and SmartFusion2 devices support secure remote upgrades with a robust IAP service using encrypted bitstreams, provide services for encrypting other boot processes, and implement mitigation techniques to protect from 'down-version' attacks. For more details on the techniques used to securely update your design remotely once it is deployed in the field, refer to the material listed in the "To Learn More" section at the end of this paper.

System Decommission

During decommissioning, the product must be disposed of so that no sensitive information is exposed to a possible attack and so that secure devices can't be reinserted into the supply chain.

An automated decommissioning process can provide a low-cost high-assurance method to decommission and account for most devices in a less-trusted environment, such as a repair depot. The automated system can use zeroization to securely erase all sensitive data, a CoC to prove erasure has been performed authentically, and a Certificate Revocation List (CRL) to prevent decommissioned devices from being reintroduced into the supply chain.

Microsemi IGLOO2 and SmartFusion2 devices support secure decommissioning with a zeroization service, an extensive CoC capability, and CRL support along with a variety of anti-tampering features to limit exposure to attacks during the decommissioning phase.

Conclusion

Protecting an embedded system during all phases of its lifecycle requires a secure root-of-trust device with DPA-resistant security key loading and storage features, that uses encrypted configuration bitstreams, and supports a secure boot, Certificate of Conformance, extensive anti-tamper protection features, and Certificate Revocation List management. Microsemi IGLOO2 and SmartFusion2 devices support all these requirements along with many more advanced security features to deliver the most secure embedded system possible. Microsemi has collected a wide range of security related material on its Security website. We invite you to visit the site to learn more about the security threats to your embedded system and the full solutions Microsemi has assembled to help you successfully implement secure systems.

To Learn More

Secure Supply Chain

1. Securing Your Supply Chain Life Cycle
2. Secure Architecture in Microsemi FPGAs and SoC FPGAs—An Overview

Secure Programming and Manufacturing

1. It's Easy to Protect Your Embedded System from Theft
2. How Easy is it to Secure Your Designs?
3. What is Design Security in a Mainstream SoC Chalk Talk

Secure System Deployment and Upgrades

1. Introduction to the SmartFusion2 and IGLOO2 Security Model
2. Overview of Secure Boot with Microsemi SmartFusion2 SoC FPGAs
3. SmartFusion2 and IGLOO2 Cryptography Services

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo CA 92656 USA
Within the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996

Microsemi Corporation (NASDAQ: MSCC) offers a comprehensive portfolio of semiconductor solutions for: aerospace, defense and security; enterprise and communications; and industrial and alternative energy markets. Products include high-performance, high-reliability analog and RF devices, mixed signal and RF integrated circuits, customizable SoCs, FPGAs, and complete subsystems. Microsemi is headquartered in Aliso Viejo, Calif. Learn more at **www.microsemi.com**.

55900160-0/11.13