Secure Boot

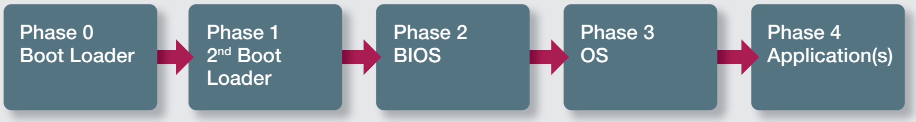
Protecting the Machines: Solving Processor Vulnerabilities

We hear of security breaches in the news every day. Primarily because most electronic systems embed processors that do not validate code before its executed. Executing un-trusted code is what creates most of the problems we hear of in the news. This represents significant vulnerabilities to applications, systems, infrastructure as well as personal data. Microsemi's Secure boot reference design can add security to a processor that doesn't have any security built-in. In addition it can prevent root kit installations if used properly.

Microsemi's Secure Boot Reference Design can uniquely solve this problem due to three simple facts:

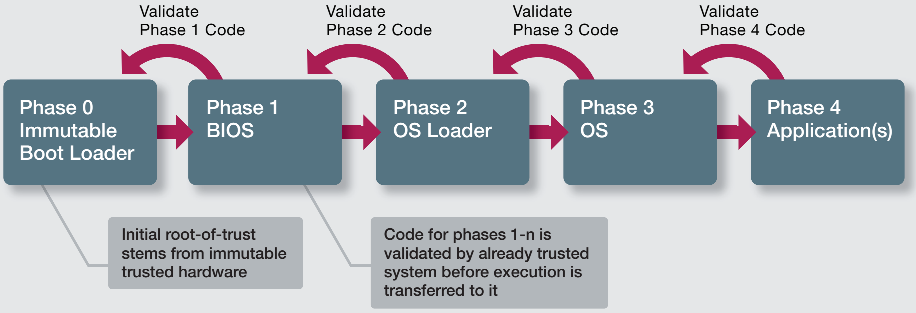
1. The worlds most secure SoC FPGA is used in conjuction with WhiteBox$^{\text{CRYPTO™}}$ to add security to a processor that has none
2. Internal secure flash memory (eNVM) can be used for storing 2nd stage boot and can be write protected to prevent rootkits from being installed
3. Fast I/Os and fast programmable logic which can emulate any memory interface that a processor needs, at speed

Processors without Secure Boot



Most processors boot and start executing; there is no verification at all of the various boot stages. Trust has not been established and cannot be extended to connected systems.

Microsemi® Secure Boot Solution



Initial root-of-trust stems from immutable trusted hardware

Code for phases 1-n is validated by already trusted system before execution is transferred to it

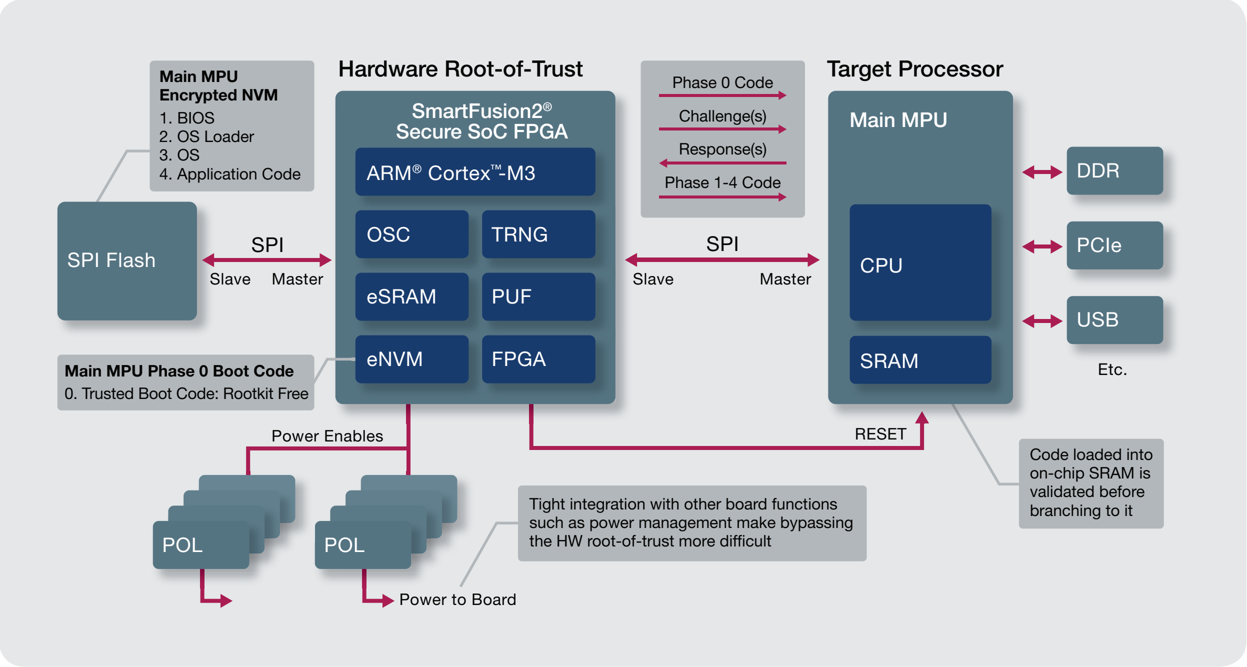
Secure boot starts from a trusted source and a process of authenticating each successive stage is performed to create a chain-of-trust as depicted in the above figure. With the Secure Boot reference design, trust can be extended to connected systems.

Microsemi

Microsemi Secure Boot Reference Design

Microsemi's reference design is enabled by its SmartFusion2 SoC FPGAs or IGLOO2 FPGAs, which offer a number of advanced security features including on-chip oscillators, accelerators for cryptographic services, secure key storage, a true random number generator, on-chip boot code storage in secure eNVM, and at-speed serial peripheral interface (SPI) flash memory emulation to enable a secure boot of an external processor at speed. The devices also feature stronger design security than other FPGAs and include differential power analysis (DPA) resistant anti-tamper measures using technology licensed from Cryptography Research Incorporated (CRI). Also included is a public instance of Microsemi's Whitebox^{CRYPTO} security product, which enables transport of a symmetric encryption key in a plain text environment through strong obfuscation.

If you have a specific need for a reference design to securely boot your processor please send an email to **socsecureboot@microsemi.com**. Please provide your contact information, and your processor part number. All downloads of Secure Boot Reference design files must be approved by Microsemi.



For further information and reference design supporting additional processors please refer to: **www.microsemi.com/products/fpga-soc/security/secure-boot**

SmartFusion2 SoC FPGAs: **www.microsemi.com/smartfusion2**

IGLOO2 FPGAs: **www.microsemi.com/igloo2**

Microsemi

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Tel: 408.433.0910 • Fax: 408.428.7896
www.microsemi.com

E-mail: Sales.Support@Microsemi.com