Infineon Security Partner Network

Infineon Security Partner Preferred

Partner Use Case

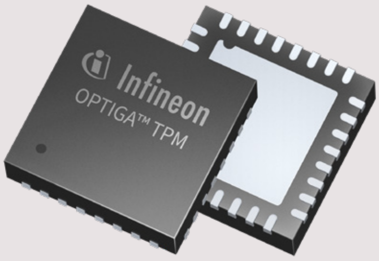
Secured Boot Implementation on Embedded ARM System-on-a-Chip (SoCs)

AVNET SILICA

Avnet Silica Software and Services offers comprehensive, custom-tailored security services, aiding customers to accelerate the implementation of embedded security on system level.

Products

SLx9670



www.infineon.com/ispn

Use case

Application context and security requirements

In the past years, adequate security protection has become a key feature of most connected products. One important factor to achieve this is securing the boot process of such devices to target that a trusted system state is established after power-on or reset. This allows to check that only software components desired by the manufacturer of the system have been executed during boot and potentially harmful additional or modified software components are hindered to run on the system.

Challenge

Different methodologies and hardware security modules (HSM) are offered by various ARM Cortex-A class SoCs to implement such a trusted and authenticated boot. However, these are custom, proprietary, unstandardized and mostly uncertified mechanisms that often require adaptions and re-certifications when moving to a different device generation, device family or device vendor. Usually, parts of the software code used in such implementations are not publicly available for review and the overall number of users of each solution offering is relatively small. These and other factors have contributed to the fact that severe security flaws have been exposed in such solutions in the recent past.

Implementation

Introducing Trusted Platform Modules (TPMs) very early in this boot process as a vendor-neutral, standardized, pre-certified trusted component helps to standardize and unify the boot process over multiple vendors or devices. However, without using an external attestation authority (usually not available in embedded systems), TPMs cannot generate a root-of-trust on such systems from which the chain of trust for the consecutive boot components is derived. Moreover, the execution speed of cryptographic algorithms such as hashing or encryption in TPMs is insufficient to be used on larger data, so a combination of TPMs, measurable software crypto implementations and HSMs (Hardware Security Modules, present on the SoC) need to be used to achieve an ideal solution.

Benefits for the user

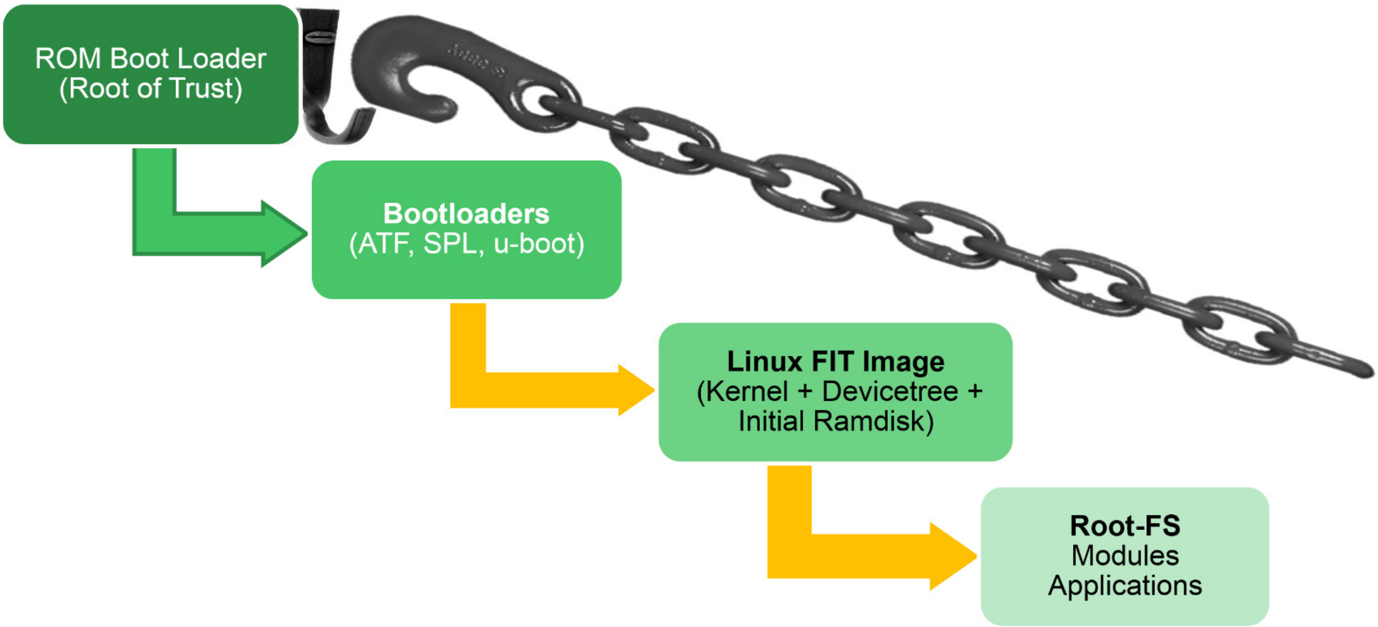
- The concept combines the strengths of all abovementioned individual components to compensate weaknesses of the respective others in a ready-to-use implementation.
- All TPM and software cryptography code is kept within a common code base, supplemented with smallest-possible additions (continuously updated and adapted to vendor flow changes and adaptions) to leverage the individual HSM modules and root-of-trust concepts of the supported SoCs.
- This keeps the custom trusted computing base to the absolute minimum and simplifies certification.
- Standardized ARM platform boot components such as u-boot Secondary Program Loader (SPL) or Trusted Framework for ARM (TFA) are extended to support trusted boot of the Linux Kernel using TPMs. Therefore it can be flexibly integrated into existing development flows or build systems.
- In user space, the chain of trust can be extended with standardized stacks to enable measurement or securing storage on application level.

Solution

Functional details and extent of trusted boot implementations are highly dependent on the individual application, security, and SoCs requirements. In the described solution, u-boot's SPL is used as the standardized entry point to TPM-based measurement of subsequent boot components. This means, that the SPL itself needs to be measured and authenticated using the SoC internal root-of-trust functionality (usually realized using the SoCs HSM), therefore providing a clean handover point between custom HSM and standardized TPM functionality. In SoCs permitting adaptions to the internal first stage boot loader, the TPM initialization can even be moved up to this level. Once the SPL is established as an element in the chain of trust and is booted, it initializes the TPM and measures its integrated software-based hash and extend function. This function is then used to subsequently measure the next components in the chain of trust, such as u-boot, TF-A, u-boot environment, device trees or the Linux Kernel, step-by-step. U-Boot commands are implemented to automate and simplify the measure-extent process for multiple binary blobs. At any defined stage, a policy tied to a specific Platform Configuration Register (PCR) measurement value in the TPM can be used to reveal keys, e.g. to decrypt subsequent components in the boot chain, such as a u-boot Flattended uImage Tree (FIT) image or the root file system partition. The concept allows to implement individual flexible solutions, but provides a standardized way of moving along the chain of trust. Yocto layers are provided to simplify configuration and building of boot and root file system components.

Main benefits of the Infineon product

Infineon's SLB9670 TPM implements the latest Trusted Computing Group (TCG) TPM 2.0 specification that provides an up-to-date toolbox of state-of-art cryptographic functions to perform a trusted boot. Due to its support for both Serial Peripheral Interface (SPI) and Inter-Integrated Circuit (I2C) interfaces it offers a great flexibility and can be connected to virtually all ARM-based SoCs. In addition, with derivatives supporting extended temperature ranges and various industrial usage profiles (such as consumer, industrial or automotive), it can support a wide range of embedded applications.



Exemplary Secure Boot Flow implemented on an ARM SoC for a Customer

Partner Use Case

Infineon Security Partner Preferred

Partner

AVNET SILICA

Partners from the Infineon Security Partner Network help you secure your devices and applications: understand which threats can undermine your business, propose solutions that will protect your business, build and implement such security solutions and, when relevant manage their operation. They have been selected by Infineon on the basis of their system security competence and ability to design and deliver strong and trustworthy security solutions. Their activities are diverse and include security consulting, security solution provision, electronic design, systems integration and trust services management. For some, offers are off-the-shelf; while for others, offers are custom-built.

Avnet Silica
The company Avnet Silica is the European semiconductor specialist division of Avnet, Inc., one of the leading global technology distributors and acts as the smart connection between customers and suppliers. The distributor simplifies complexity by providing creative solutions, technology and logistics support. With a team of more than 200 application engineers and technical specialists, Avnet Silica supports projects all the way from the idea to the concept to production. Fifteen thousand customers throughout Europe are convinced of our service quality – in respect of both technology and logistics, not least because our application engineers focus on solution-oriented „design in“ consulting and technical product support.

Avnet Silica’s contribution to the Infineon Security Partner Network
The Avnet Silica “Software and Services” department offers security trainings to bring end-users up to speed on system-level security including both, hardware and software aspects.
To cover topics in even greater detail, consultancy services are offered on

- Threat analysis and modeling
- Implementation of security concepts
- Implementation of specific features or threats countermeasures
- Software/system level security concepts

In this role, the “Software and Services” department advises and complements customers’ own engineering teams for the specification and development of the respective solution. On top, Avnet Silica software engineering resources are available upon request to work with and complement customers’ own engineering teams for the respective solution implementation. To ease transition into production, Avnet Silica offers personalization and provisioning services for Infineon security solutions.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 06 / 2019

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (www.infineon.com).

Please note!
THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND ANY INFORMATION GIVEN HEREIN SHALL IN NO EVENT BE REGARDED AS A WARRANTY, GUARANTEE OR DESCRIPTION OF ANY FUNCTIONALITY, CONDITIONS AND/OR QUALITY OF OUR PRODUCTS OR ANY SUITABILITY FOR A PARTICULAR PURPOSE. WITH REGARD TO THE TECHNICAL SPECIFICATIONS OF OUR PRODUCTS, WE KINDLY ASK YOU TO REFER TO THE RELEVANT PRODUCT DATA SHEETS PROVIDED BY US. OUR CUSTOMERS AND THEIR TECHNICAL DEPARTMENTS ARE REQUIRED TO EVALUATE THE SUITABILITY OF OUR PRODUCTS FOR THE INTENDED APPLICATION.

WE RESERVE THE RIGHT TO CHANGE THIS DOCUMENT AND/OR THE INFORMATION GIVEN HEREIN AT ANY TIME.

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life-endangering applications, including but not limited to medical, nuclear, military, life-critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.