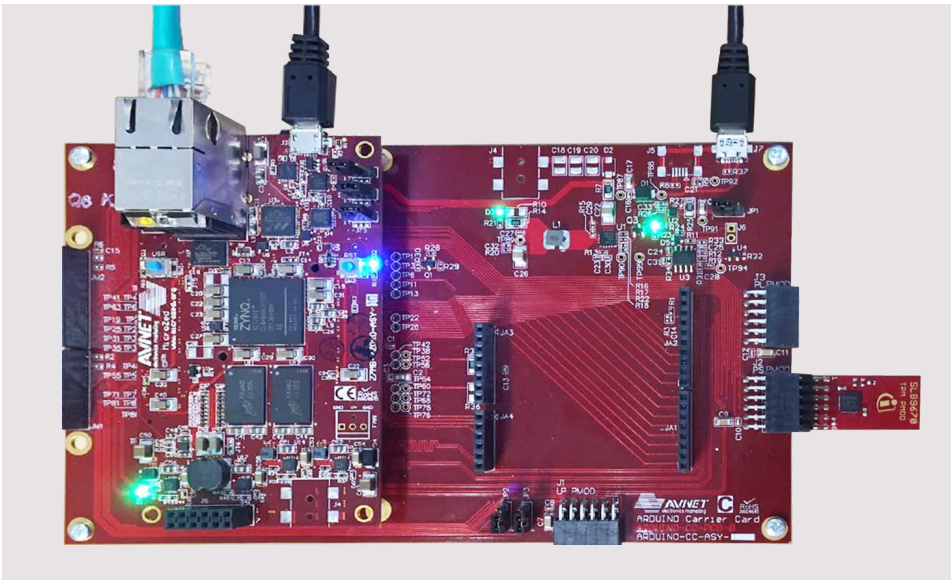
Security Partner

Partner Use Case

Measured Boot of Zynq®–7000 All Programmable SoCs

XILINX ALL PROGRAMMABLE™

Measured boot augmenting secured boot in connected, upgradable systems is a critical component of cyber security in Industrial IoT and other applications.



Products

OPTIGA™ TPM

Use case

Application context and security requirement

Software updates and remote attestation require a secured connection between a server and the embedded system clients. Typically, the network has a large attack surface because it can be attacked by any adversary with access to the Internet. For firmware updates, a server to client(s) connection is used. In some factory automation environments, client-to-client communication is also needed to coordinate operational procedures.

Challenge

In most current applications, Xilinx field programmable gate arrays (FPGAs) and system on chips (SoCs) are programmed once at the factory and not reconfigured for the life cycle of the device. A method to add functionality and/or reduce the total cost of ownership (TCO) of an embedded system is to support field updates. Field updates are typically done over the Internet, which opens up attacks on an embedded system to anyone with network access.

Implementation

With field updates over the internet susceptible to attacks, measured boot and network security are critical in firmware updates. In Zynq®-7000 All Programmable (AP) SoCs, the SoC and programmable logic can be updated, so field updates can be very effective to add, upgrade and update functionality and reduce total cost of ownership.

Benefits for the user:

Measured boot is done in addition to secured boot. The OPTIGA™ Trusted Platform Module (TPM) enhances the hardware root of trust (HROT) and increases the security of the software loaded and update process. As the HROT is enhanced with the TPM, an adversary would have to defeat both the Zynq-7000 AP SoC and the tamper-resistant TPM in order to carry out a successful attack.

Security Partner

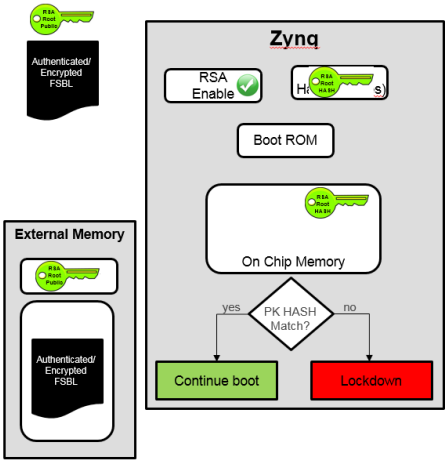
Solution

The secured boot functionality for the Zynq®-7000 All Programmable (AP) SoC provides the capability to authenticate all partitions loaded at boot using RSA-2048 authentication. It also supports advanced encryption standard (AES) encryption of partitions that need confidentiality. The Zynq-7000 AP SoC BootROM includes security functions to provide a hardware root of trust (HROT) to protect against early load attacks. This solution discusses a method to add measured boot capability to Zynq-7000 AP SoCs used in a connected environment. A server provides remote attestation that the embedded systems boot with trusted software over a secured network. The method uses an Infineon OPTIGA™ TPM to enhance the HROT functionality. The solution described is available as an application note (XAPP1309) and reference design, which can be found on xilinx.com and features the Xilinx Zynq®-7000 on the Avnet Industrial IoT Starter Kit paired with an Infineon OPTIGA™ TPM Pmod accessory for the kit. Both the Kit and the Pmod are available at microzed.org.

The OPTIGA™ TPM provides partition measurements, cryptographic functions, and secured key storage in a cost-effective, tamper-resistant device which are an effective complement to Zynq-7000 SoC security functions.

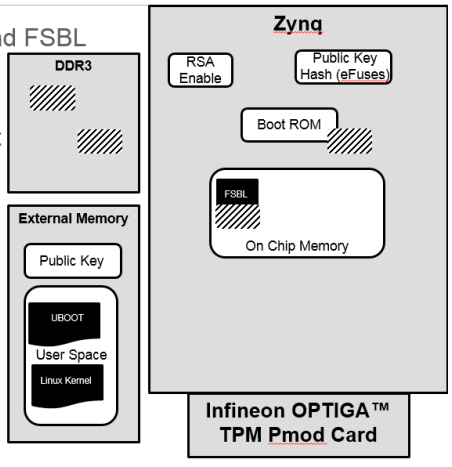
Existing Zynq Root of Trust Boot

- Step 1: Provision Device Before
  - Load your RSA-2048 public key HASH into device
  - Load your public key into Flash
  - Load your signed FSBL into Flash
  - Turn On Root of Trust Boot
- Step 2: Field System
- Step 3: Apply Power, ROM Boots
  - Device loads public key from Flash into OCM
  - Device calculates HASH of public key
  - Device compares calculated HASH vs stored HASH
    - If successful – load, authenticate/decrypt and execute FSBL
    - If failure – go into Secure Lockdown and notify system



New Measured Boot Capability with TPM

- Step 4: FSBL Measures and Extends Boot ROM and FSBL
  - Hash code
  - Send hash to TPM with Extend command
- Step 5: FSBL Measures, Extends, and Runs u-boot
  - Hash code
  - Send hash to TPM with Extend command
  - Run code
  - Decryption and authentication is optional here
    - Left up to the customer
- Step 6: Boot Sequence Continues
  - Each Stage Measures, Extends, and Runs the Next
  - Decryption and authentication is optional here
    - Left up to the customer



Security Partner

Partner

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.

Xilinx

Xilinx is the world's leading provider of All Programmable FPGAs, SoCs and 3D ICs. These industry-leading devices are coupled with a next-generation design environment and IP to serve a broad range of customer needs, from programmable logic to programmable systems integration. Xilinx devices are used in Aerospace & Defense, Automotive, Broadcast & Pro A/V, Consumer, Data Center, Industrial & IIoT, Medical, Test & Measurement, Wired and Wireless Communications applications. Xilinx devices are used in customer platforms that benefit from higher performance, lower power, multi-protocol communication, precision control, robust security, functional safety, or other forms of customization beyond what is available in application-specific standard products (ASSPs) with a lower total cost of ownership than application specific integrated circuits (ASICs). Headquartered in San Jose, California, with locations around the world, Xilinx has over 3,500 employees and 20,000 customers. For more information, visit www.xilinx.com.

Xilinx's contribution to the Infineon Security Partner Network

Xilinx is proud to be the first System-on-Chip (SoC) provider in the Infineon Security Partner Network. The Zynq® family of Xilinx All Programmable SoCs include the hardware root of trust (HRoT) for secure boot. In order to create a highly secured, connected, and upgradable system, as required for the Industrial Internet of Things (IIoT), Xilinx has partnered with Infineon and Avnet to create a measured boot with remote attestation application note and reference design.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 07 / 2017

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).