TPM Assisted Security for FPGAs

Ali Shuja Siddiqui, Yutian Gui, Jim Plusquellic* and Fareena Saqib
Dept. of Electrical Engineering, University of North Carolina at Charlotte and University of New Mexico
asiddiq6@uncc.edu, ygui@uncc.edu, jimp@ece.unm.edu*, fsaqib@uncc.edu.

Motivation

Field Programmable Gate Arrays (FPGA) provide reconfigurable hardware that can be updated on the fly with changing requirements. FPGA based hardware vendor's use this ability to provide end users with hardware updates. FPGA manufacturers currently provide encryption and authentication of bitstream through AES and RSA. However, the implementation is limited in scope. On Xilinx's FPGA boards there are two storage areas for holding encryption keys on non-volatile and one-time programmable fuses or on battery powered RAM. Battery powered RAM allows for volatile keys, but it also requires a battery to be always installed. Using well established constructs such as Trusted Platform Modules (TPMs) can be used to offload security, thus overcoming the restrictions of on-board security.

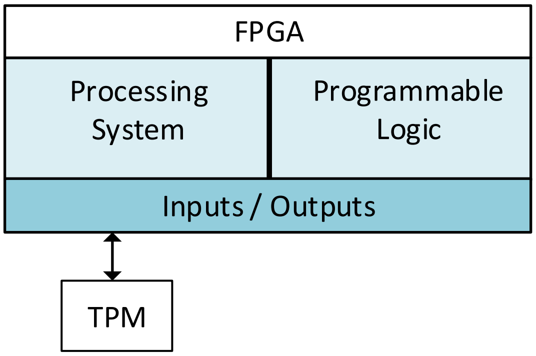

Figure 1: Block diagram of the demo system.

Background

Trusted Platform Modules are crypto-processors that are connected to a host system. Current generation of TPM is 2.0. It is built on top of its predecessor specification, 1.2. In addition to basic security functions such as RSA and SHA1 encryption, TPM 2.0 adds Elliptic Curve Cryptography, key pair generation, current generation hashing algorithms such as SHA256, as well as provides higher level of security functions such as Secure-boot, data sealing and data attestation. Unlike its alternative, Hardware Security Modules (HSMs), TPM is low cost, more commercial and highly integrable in small scale devices, e.g. Internet of Things (IoTs), industrial / military embedded systems and wireless sensor networks.

Limitations in current generation FPGA hardware and software have a narrow scope of security, as noted. TPMs when connected with FPGAs can provide an extension to the security capabilities of the hardware. Currently, the use of TPMs in the computing sphere is synonymous for enabling boot level integrity with technologies, such as Root of Trust and Secure Boot. With the help of TPMs, the same concepts can be translated to the reconfigurable FPGA domains while discarding unreliable and fragile solutions provided by the vendor. Additionally, TPMs can also provide a plethora of proven and tested secure functions to the hardware, which otherwise would have been needed to be implemented on the fabric. A process that not only consumes limited on-board resources, but also requires additional work on the part of the designer to ensure that the implemented security function is indeed secure.

Demo Objectives and Observables

We demonstrate integration of TPM module with FPGAs. TPM based functions are used to show how security is improved for FPGAs for bitstreams, code and the running hardware and software application. Figure 1 details block diagram of our target system. The demo presents various threat models and propose a secure framework to enhance the security of reconfigurable framework. The setup of the demo is shown in figure 2.

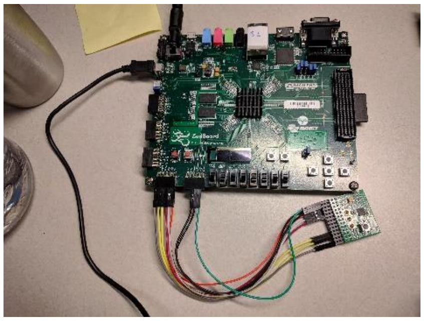

Figure 2: Demo Setup.

Hardware Used

- Reconfigurable logic design based on Xilinx Zynq 7000 Zedboard
- Trusted platform module TPM2.0

Goal

The demo will demonstrate advanced features of trusted platform module integrated with the reconfigurable platform for secure and reconfigurable designs.