Partially reconfigurable TPM Architectures as the Security Anchors of future Embedded IT Systems

Sunil Malipatlolla[1], Thomas Feller[2], and Sorin A. Huss[1, 2]

[1]Center for Advanced Security Research Darmstadt (CASED), Darmstadt, Germany
[2]Integrated Circuits and Systems Lab, Technische Universität Darmstadt, Germany

Email: huss@iss.tu-darmstadt.de

Abstract

Currently, commercial embedded systems are increasingly exploiting reconfigurable devices such as Field Programmable Gate Arrays (FPGAs). Due to the volatile nature of SRAM-based FPGAs it is necessary to secure such systems against intellectual property theft and product piracy. As an additional requirement, the trustworthy operation of these systems has to be monitored in order to protect the processed, and in many cases sensitive, data. Trusted Platform Modules (TPMs) are in general intended to be used for trustworthy attestation; they thus form the security anchors of such systems. A TPM is microcontroller-based chip, which provides additional hardware-based security to the user's data, cryptographic keys, and other secrets. For this purpose, the TPM is equipped with hardwired cryptographic engines such as RSA, SHA-1 and HMAC that rely on correspondingly uncompromised cryptographic algorithms. Therefore, in case of a compromised RSA algorithm, not only the data protected by the TPM is lost, but also the generated signatures become invalid.

One possible solution to this problem is to replace (i.e., update) the encryption engine on the TPM with a new, uncompromised asymmetric engine (e.g., ECC). However, current TPMs are in general embodied as Application Specific Integrated Circuits (ASICs) only, thus they cannot be modified after production and deployment.

In this contribution we propose a novel architecture, referred to as Update Architecture (UA), which supports a secure update of TPM cryptographic engines. The proposed architecture takes the generic SRAM-based FPGA architecture as a foundation, which supports a dynamic, i.e., runtime, partial reconfiguration of functionality. Such FPGAs may be upgraded accordingly in order to communicate with both embedded and external non-volatile memory (NVM) modules in a secured way. In addition to providing both secure update and NVM communication, this approach provides additional methods aimed to regain trust in the system, which is mandatory for a subsequent operation of the system after a TPM update. A proof-of-concept implementation of the proposed architecture is demonstrated for the Xilinx Virtex-5 FPGA platform.