zTPM : A New Hardware Architecture for TPM in Embedded Virtualization

Franck Bucheron [1,2], Arnaud Tisserand [2] and Louis Rilling [1]
[1] DGA, [2] CNRS-IRISA-INRIA-UR1

Today, processors for embedded systems can efficiently support virtualization. But even with a high isolation and protections against software attacks, embedded systems have also to face hardware attacks such as side channel attacks (SCAs). Hence, virtualization for embedded systems requires a combined hardware/software (HW/SW) codesign approach.

In this paper, we first discuss specific features and requirements of secure embedded systems, existing solutions for implementing virtualization and defining sufficient levels of security. We also present up-to-date specifications to improve virtualization performances using hardware security. We also discuss the absolute need of cryptography in a secure architecture.

Second, we study a complete solution which shows requirements to get a trustworthy complete secured solution and, most important, what remaining tasks. We also present security features of our platform : a Zynq-7000 HW/SW platform composed of a processor (ARM Cortex-A9 dual-core) and a FPGA (Artix-7) in the same device.

Third, we present our HW/SW solution and we focus on some parts based on HW IPs expecting to be as close as the conformity with the 2nd version of the recommendations of the *trusted computing group* (TCG). We summarize some parts of the SW stack to avoid enlargement of the trusted computing base (TCB) of the *hypervisor*, being located in the Trustzone of the ARM processor. We also expose algorithms of a SW command validation, choice of a *virtual trusted platform module* (TPM), ways to calculate the worst case execution time (WCET) of a command, deadlocks between different components of our IPs.

In a last part of this paper, we summarize the future developments.

The proposed HW architecture and SW stack will allow the end user to launch *virtual machines* (VMs) where the executed code is trusted (*i.e.*, verified and the user is granted) and the manipulated data are also trusted (*i.e.*, integrity is ensured and only authorized users have access to these data inside the complete HW/SW platform).