Hardware Demo Proposal

Implementing Trusted Computing Design for IoT

Edumund Ahovi, Khir Henderson , Denzel Hamilton, and Kevin Kornegay

Morgan State University, Baltimore, Maryland,
Department of Electrical and Computer Engineering,

This hardware demonstration is an application of trusted computing design for IoT devices and embedded systems using security protocols and procedures provided by the trusted platform module (TPM). TPM is a hardware security standard developed by the Trusted Computing Group that is used to establish trust in computer networks. In this demonstration we will use TPM hardware to support remote attestation to prevent a firmware roll back attack which occurs when a device manufacturer provides a software update to fix a known security vulnerability, then the attacker circumvents the software security and rewrites an older version of the unpatched software. We will use a Xilinx ZCU102C application development board, which includes a Zynq UltraScale+™ MPSoC equipped with crypto engine, secure memory to secure keys and hardware to generate certificates to establish a trusted link between an update server and IoT device. Remote Attestation is a method where hardware and software combine with a remote party to create a layer of trust. The procedure is shown below.

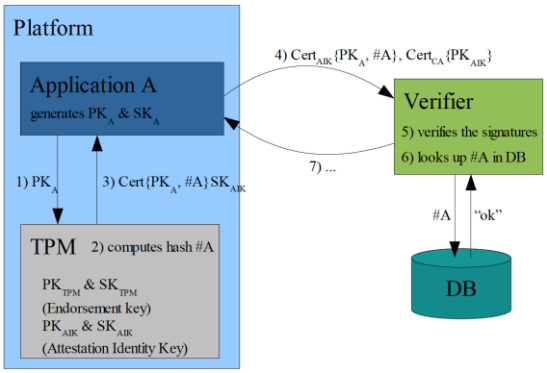


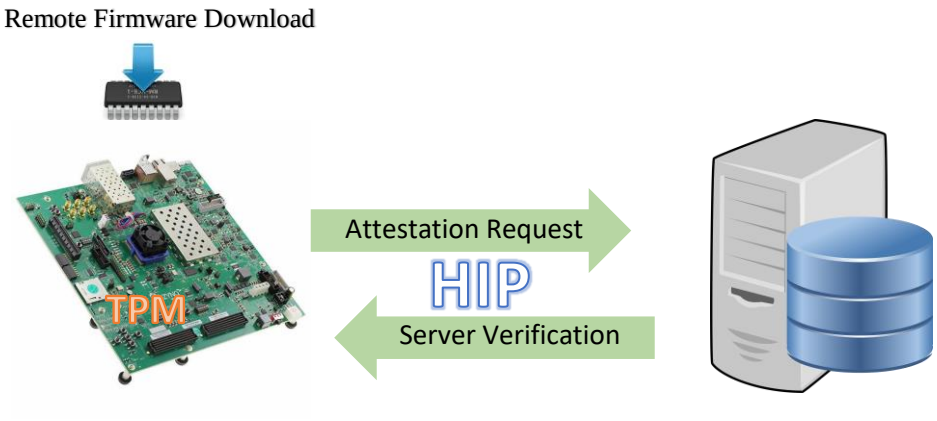
Figure 1 - Remote Attestation Process

The remote attestation protocol used shown in Figure 1 is briefly described in the following steps.

1. Application in the form of firmware "A" generates a public/private key pair PK_A and SK_A stored into the secure memory of a TPM and then asks to be certified.
2. TPM computes a hash tag #A of the executable code of program "A".
3. TPM creates a certification including PK_A and #A and signs it with the attestation identity key SK_{AIK}.
4. When application "A" wishes to authenticate itself to a remote party, it sends the cert. of its public key and hash value #A along with a cert. issued to the TPM by a trusted certification authority (CA).
5. The remote party verifies the cert. chain. Over HIP
6. The remote party looks #A up in a database which maps hash values to trust levels.
7. If application "A" is deemed trustworthy, we continue the communication using PK_A to establish a session key.

Experimental Setup

The observable demonstration intends to be informative, directly walking through each step of the attestation process. A major goal is to support the implementations of hardware security and procedures built into IoT devices. The demonstration requires a computer used as the update and verification server and command and control, and the ZCU102 board that is configured as a lightweight IoT device. The demonstration will use two monitors to show the encoding and verification processes as well as the results of a tampered and untampered firmware application. The results will be presented on a poster. The poster will also explore design feasibility as well as cost and ease of implementation into IoT devices and effectiveness of TPM hardware attestation in IoT devices.



REFERENCES

[1] Coker, G., Guttman, J., Loscocco, P., Herzog, A., Millen, J., O'Hanlon, B., Ramsdell, J., Segall, A., Sheehy, J. and Sniffen, B. (2011). Principles of remote attestation. *International Journal of Information Security*, 10(2), pp.63-81.

[2] Gurtov, A. (2008). *Host Identity Protocol (HIP)*. Chichester: Willey.

[3] Moskowitz, R. and Nikander, P., "Host Identity Protocol Architecture," RFC 4423, May 2006.

[4] Ultrascale MPSoC ZCU102 Eval Kit." Xilinx MPSoC Evaluation Kit. Xilinx, n.d. Web. 24 Oct. 2016

[5] V. Haldar, D. Chandra, and M. Franz. "Semantic Remote Attestation A Virtual Machine directed approach to Trusted Computing". *USENIX Virtual Machine Research and Technology Symposium*, May 2004.

[6] W. Arthur, D. Challener and K. Goldman, *A practical guide to TPM 2.0*.