Mike Mishal

mmisha2

Report 6

03/9/2019

Papers Read:

1. FPGAs for trusted cloud computing

This paper explains a security risk in the cloud computing for storing sensitive data. As secure data is transferred to the cloud using SSL, it resides as plain text on the resource until it is encrypted and tokenized. They suggest a trusted compute resources to store keys, encrypt, decrypt, and perform authentication. They suggest to use FPGAs as the trusted compute recourse because they are more secure (isolated memory space) and has better performance.

The system Architecture contains a trusted authority that generates a random symmetric encryption key that is copied to the FPGA on board memory. (can we use side channel to read it?) another option is for the TA to generate a public/private key unique to each device and place the private key into the bootstrapping binary and publish the public one. Using the symmetric key, the binaries can be encrypted and transferred to the device. The client connects to the FPGA using the public key similar to SSH sessions.

1. On the security Evaluation of the ARM TrustZone extension in a heterogeneous SoC

This paper presents relevant attack scenarios based on third party IP to exploit some security failures of the TrustZone extension on SoC. The analysis is on Zynq-7010 FPGA SoC. It assumes that the attacker has access to the RTL code and can change it.

Attack #1: Make changes in the design before the AXI interconnect on the PL side and fixes the signal to low.

Attack#2: Same as #1 but fixes the signal to high creating a DoS attack.

Attack#3: PL responds with OKAY to all requests. No SLVERR or DECERR.

Attack#4: PL responds with SLVERR or DECERR to all requests. (DoS)

Attack#5: Adds a FIFO to the AXI Interconnect that stores data. (Very interesting)

Attack#6: Uses a malicious IP with a memory-mapped master port to have a direct access to DDR3. The attack bypasses almost all security measures.

Design Recommendation#1: Create two AXI interconnect, one for each world. Security checking on PS side

Design Recommendation#2: Use HP port to connect to all non-sensitive memory-mapped master interface. Checking is done on the PS side as well as the PL.

Countermeasure#1: Use memory protection (Zynq Ultrascale+.

Countermeasure#2: Apply cryptography operations to all read and write to the external memory.

Countermeasure#3: Use Input-Output Memory Management Unit (IOMMU) to protect from faulty or malicious devices.

Papers to Read:

1. The Security of ARM TrustZone in a FPGA-based Soc
2. Secure FPGA as a Service – Towards Secure Data Processing by Physicalizing the Cloud

Current Interest:

Differential power analysis attacks on ARM protected world in FPGA-CPU systems.