Intel FPGAs Security Bootcamp

Course Description

FPGAs are widely used in many areas, including automotive electronics, avionics, medical devices, military and consumer electronics, large scale cloud, data centers and is gaining more and more popularity.

FPGA security becomes an issue because adversaries can:

- Reverse engineer FPGA design to steal valuable IP information
- Obtain decrypted FPGA bitstream by wire-tap
- Clone FPGAs/IPs and sell them
- Use replay attack on the previous system version with vulnerabilities
- Conduct remote side channel attacks without physical access (cloud, data center, SoC)
- Attack hardware by software and software by hardware
- Insert hardware Trojan as a backdoor
- Cause denial of service

FPGA vendors try to address security threats by providing a set of features protecting the device and the user application availability, confidentiality and integrity.

This 3-days training provides all necessary theoretical and practical know-how to secure modern SoC FPGA-based systems, and help customers not just to understand the concepts but also how to implement and integrate them into their project.

The training starts by introducing the main security threats that may be encountered by application designers when working on FPGA.

The training continues by describing the security building blocks currently provided by the Intel, and the role of each one of them.

The security techniques are demonstrated using recent, state of the art Intel’s Agilex SoC FPGA family.

Course Duration

3 days

Goals & Objectives

1. Become familiar with FPGA & SoC FPGAs security threats
2. Describe the FPGA & SoC FPGA security concepts
3. Become familiar with Intel's security building blocks role and when to use each one of them
4. Apply countermeasures with modern FPGA & SoC FPGA
5. Design a complete secure boot flow (including ARM TrustZone)
6. Analyze security overhead in your project (timing, area, power)
7. Design defensive layers to protect hardware attacks on Arm processors and FPGA logic
8. Apply best design practices for a complete FPGA & SoC FPGA secure flow
9. Be able to apply security to your projects

Intended Audience

FPGA and firmware engineers, beginners or experienced, that would like to design secured FPGA & SoC FPGA based systems, and apply the recommended secured design flow for hardware and software.

Perquisites

FPGA & SoC FPGA architecture, basic SoC FPGA design, VHDL/Verilog

Course Material

- A digital copy of all lecture slides

Table of Contents