



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL

altera™ solution
acceleration partner



Agilex FPGA Security

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 4-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.



When innovation meets expertise...



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL

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 discussed & demonstrated through practical hands-on labs using state of the art Altera Agilex SoC FPGA family and Quartus Prime Pro.

Each attendee receives an official certificate from Altera and from Arm (Exam must be passed).

Course Duration

4 days

Goals

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

Intended Users

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

Prerequisites

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

Course Material

- Course book
- Lab handbook + lab files
- Quartus Prime Pro
- Linux OS



When innovation meets expertise...

Table of Contents

Day #1

❖ Introduction to FPGA security

- Security implications of FPGAs
- What makes FPGA vulnerable?
- Case studies of FPGA vulnerabilities
- Protecting FPGA assets
- FPGA SoC assets
- Hardware security vs hardware trust
- Threats to the FPGA development lifecycle
- Challenges in FPGA security
- FPGA security assumptions
- Old vs modern FPGA security
- Security design challenges

❖ Basic Security Concepts

- Basic security requirements
- How security requirements are mapped to FPGAs?
- Security terminology
- The threat relation
- Threat actors
- FPGA attack surface
- FPGA attack vectors
- Local vs remote attack vectors

❖ FPGA Security Threats Landscape

- FPGA threat landscape
- FPGA attacks through lifecycle
- Attacker's arsenal state-of-the-art tools
- FPGA bitstream attack taxonomy
- IP theft attacks
- Cloning attacks
- Bitstream readback attacks
- Bitstream eavesdropping attacks
- Bitstream probing attacks
- Side Channel Attacks (SCA)
- Electromagnetic field analysis
- Stealing decryption key from eFUSE
- Stealing decryption key during FPGA upgrade
- Reverse engineering attacks
- IP overbuilding attacks
- IP tampering attacks
- Fault Injection (FI) attacks
- Hardware trojan attacks
- Replay attacks
- Denial of Service (DoS) attacks
- Case studies from modern FPGA attacks

❖ SoC FPGA Security Threats Landscape

- Introduction to SoC FPGA

- Common attacks on SoC FPGA
- Attacks from FPGA on processor core
- Attacks from processor core on FPGA
- Attacks on memory and peripherals
- Case studies from modern SoC FPGA attacks

Day #2

❖ **Cryptography 101**

- The goal of cryptography
- Cipher algorithms leakage
- Randomness
- Use of encryption
- Cryptographic Hash functions
- Hash Based Message Authentication Codes (HMAC)
- Symmetric key cryptography
- AES encryption/decryption and modes
- Asymmetric key cryptography
- Asymmetric vs symmetric cryptography
- What is Key Derivation Function?
- Key Exchange Algorithms
- The RSA algorithm
- Elliptic Curve Diffie Helman
- Digital signature
- Digital certificates
- Using certificates against MITM attacks



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL

- Encryption key management
- Post Quantum Cryptography (PQC)

❖ **Modern FPGA Defenses & Countermeasures**

- SoC FPGA modern security primitives
- FPGA cryptographic services
- Bitstream encryption
- Red key vs black key concept
- Bitstream authentication
- Breaking bitstream encryption
- Watermarking & fingerprinting mitigations
- Logical obfuscation mitigations
- Disabling readback
- Physically Unclonable Function (PUF)
- Black key provisioning using PUF
- Cloning mitigations
- Replay attack mitigations
- IP overbuilding mitigations
- Hardware trojans mitigations
- Hardware trojans detection methods
- Partial reconfiguration bitstream security verification
- Debug authentication
- Trusted Platform Module (TPM)
- Integration of external TPM to FPGA as FSBL (First Stage Boot Loader)
- Hardware Security Module (HSM)



When innovation meets expertise...

- HSM vs TPM
- Bitstream key generation storage strategies
- Reverse engineering mitigations
- Physical anti-tamper mitigations
- Fault injection countermeasures
- Zeroization mechanism

Day #3

❖ **FPGA SoC Security**

- FPGA SoC booting stages
- FPGA SoC booting modes
- SoC secure boot
- Remote attestation & Measured boot

❖ **FPGA SoC Security Architecture**

- FPGA SoC general architecture & attack surface
- Attacks on Firmware software
- MMU & IOMMU/SMMU
- Security by isolation
- Trusted Execution Environment (TEE)
- Hardware support for TEE
- Arm TrustZone for Cortex-A Processors
- Muti-core topology
- Boot example
- Armv8-A boot sequence

- What is AMBA AXI?
- How the AXI bus is used in FPGA SoC?
- Virtualization & containerization

Day #4

❖ Securing FPGA Data at Rest

- FPGA and FPGA SoC memory protection introduction
- Sources of attacks on memory
- Types of attacks on memory & mitigations
- DMA attacks
- Rowhammer and Jackhammer attacks
- Cold boot attack
- Confidentiality protection
- Integrity protection
- Memory access pattern protection
- Security of non-volatile memories
- NVRAM consistency challenge

❖ Securing FPGA Data in Motion

- Introduction to network security
- Choosing the network layer for security
- Relying on data-link protection only
- Use case: IPSec protocol
- Use case: TLS protocol
- IPSec vs TLS

- Intrusion detection & security monitoring techniques

❖ Altera Agilex Family Security

- High-level security features in Agilex 3/5/7
- Agilex 3/5/7 processor system
- Agilex 3/5/7 NoC
- NoC segments for security
- AXI4 protocol, QoS, and fabric NoC considerations
- NoC design considerations
- Agilex 3/5/7 secure boot
- Security mechanisms in secure boot
- Agilex 3/5/7 Runtime security mechanisms
- Priority scrubbing
- Secure monitor and service layer
- Security Device Manager (SDM)
- Secure debug
- Key storage and management
- Cryptographic hardware accelerators

❖ Security Implications on FPGA

- Implications of security mitigations
- How security affect FPGA performance?
- How security affect FPGA area?
- How security affect FPGA power consumption?
- How security affect FPGA boot time?
- Tips to reduce security implications



OREN HANDS ON TRAINING & DEVELOPMENT LTD.
20 YAIR ROZENBLUM ST. KFAR SABA 4464601 ISRAEL

❖ **FPGA Security Best Practices**

- FPGA security design review methodology
- Security standards
- FPGA security evaluation

Lab #1: Apply various security features of Agilex5 for a given design and report the effect on performance/area.

Lab #2: Implement a secure boot flow from power up till user application.

Lab #3: Apply NoC security features and run-time security features.



When innovation meets expertise...