SoC FPGA Hardware Security Requirements and Roadmap

Ryan Kenny, Strategic Marketing
Intel Programmable Solutions Group
Agenda

• Security Threat Models for FPGA/SoC FPGA End Markets

• Taxonomy of Security Threats

• Threat Use Cases

• Overall Security Product Features and Roadmap
FPGA or SoC FPGA User Markets and Threats

**COMMUNICATIONS**
- Wireless
- Networking
- Wireline

**COMPUTER AND STORAGE**
- Computer
- Storage
- Office

**DIGITAL CONSUMER**
- Entertainment
- Broadcast

**INDUSTRIAL**
- Instrumentation
- Energy
- Automotive
- Military
FPGA or SoC FPGA User Markets and Threats

COMMUNICATIONS
- Supply Chain
- Data In Transit
- Data At Rest

COMPUTER AND STORAGE
- Remote Access/Update
- Physical/Reverse Engineering

DIGITAL CONSUMER

INDUSTRIAL
Where FPGA Security Requirements Originate

Requirements (2010)

Requirements (2016)

- Military
- Industrial
- Wireline
- Computer/Storage
- Automotive
- Other
Threat Models: Industrial IoT

Threat Model
Very Complex

Primarily Remote Access, Targeting Privacy Information

Requires Hardened Identity Management and Accelerated Authentication
Threat Models: Wireline Systems

Threats are to data as well as infrastructure

Targets are both owners and users of telecommunications

Solutions require novel access controls, hardware identity, and supply chain control
Threat Models: Data Center

Platform-Specific Security Risks

Variety of Physical and Virtual Isolation Features Needed by FPGA and SoC FPGA
Data Center Security is a Variable in Cloud Adoption

Adoption of Virtualization Depends on Security Models

Security Solutions are a Combination of Cloud Architecture and 3rd Party Software

Hardware-Based Security (Identity) Difficult in Virtual Environments
Agenda

• Security Threat Models for FPGA/SoC FPGA End Markets

• Taxonomy of Security Threats

• Threat Use Cases

• Overall Security Product Features and Roadmap
Universe (Known) of Hardware Threats

**FPGA-BASED ATTACKS**

- Non-invasive
  - Side channel
  - Network
  - Boot code
  - Over-voltage
  - Over-temp
  - Clock skew
  - Single-event upset (SEU)
  - Glitching

- Invasive
  - Decap
  - FIB
  - Microprobe
  - Chemical Erode
  - Electron Microscope

**SUPPLY CHAIN ATTACKS**

- Silicon
  - Mask set
  - Clone / counterfeit
  - Boot code

- Software
  - Extra circuits

- Intellectual Property
  - Extra circuits
  - Hidden failure modes
  - Extract data and keys
Speculative New Threats

INTER-FPGA ATTACKS

PR Region

Unauthorized Partial Reconfiguration (PR)
Local Thermal Effects
PR Timing Attacks
Create Routing Violations

ENIY OF SERVICE (DOS) ATTACKS

Config

Mask set
Clone / counterfeit
Boot code

SOC

ARM* Malware to:
PR
DoS NOC

Mx

Debug DoS
Upgrade DoS

1Threats are Speculative Until Multi-Tenant FPGA Systems Develop
Agenda

• Security Threat Models for FPGA/SoC FPGA End Markets

• Taxonomy of Security Threats

• Threat Use Cases

• Overall Security Product Features and Roadmap
Security Use Case: FPGA Design Cloning

FPGA Design Cloning and Reverse Engineering

Stratix® II to Present
Encrypt Configuration
Store and Protect Key on FPGA

Mitigation

Configuration memory
Thief intercepts configuration data
FPGA
Security Use Case: Imaging or Probing Key Attack

Key Imaging or Device Reverse Engineering

Mitigation

Stratix® IV Through Arria® 10 Keys Uniquely Scrambled in Fuses

Stratix® 10 Physical Unclonable Function (PUF) Protected Keys
Security Use Case: Side Channel Key Attack

Key Extraction Using Side Channel (Power) Attack

Mitigation

Arria® 10 DPA Resistant Decryptor

Mitigation

Stratix® 10 Customizable Boot Processes
Security Use Case: Unauthorized Mx/Debug

Unauthorized Maintenance and Device Debug

Cyclone® III Through Stratix® 10
Disable JTAG and Debug Ports

Mitigation

Stratix 10
Forced Authentication of All Debug and Maintenance Inputs

Mitigation

Unauthorized Maintenance
and Device Debug

Mitigation

Cyclone® III Through Stratix® 10
Disable JTAG and Debug Ports

Stratix 10
Forced Authentication of All Debug and Maintenance Inputs
Security Use Case: Boot or Config Code Alteration

Boot or Configuration Code Alteration

Arria® 10 and Stratix® 10
Symmetric and Asymmetric Authentication
(Internal or External Root of Trust)

Mitigation
Future Security Use Case: Multi-Tenancy

PR Regions (VM Components) Can Interfere with One Another

Stratix® 10 and Beyond: Secure Isolation of Blue/Green and Green/Green Bitstreams

Device Manager Virtual Machine Monitor Device Manager

IOMMU

FPGA

Device

Device

Memory

Guest OS

Guest OS

App

App

App

App

Mitigation
Agenda

• Security Threat Models for FPGA/SoC FPGA End Markets

• Taxonomy of Security Threats

• Threat Use Cases

• Overall Security Product Features and Roadmap
Intel® PSG Roadmap of SoC FPGA Security Features

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.
Block Level Capabilities of Stratix® 10 SDM
Secure Device Manager with Configuration Sectors

• Stratix® 10 bitstreams will be ‘sectorized’ and configure sectors in parallel

• This also allows zeroization to be partial, complete, ordered, or fully parallel

• Verification can be performed likewise at the sector level

• This also enhances Error Detection Cyclic Redundancy Check and response (Scrubbing)
Configuration Flow for Stratix® 10 Device

SDM Configuration

Configuration Source (Flash/Hard Drive)

FPGA Sector and ARM Configuration

SDM Image Authenticated
- Configure SDM
- Altera Signature
- Customer Signature

Optional

Boot Order Decisions
- Sector Security Decisions
- System Integrity Decisions

FPGA Sector
- Header Signature

Encryption Optional (Separate Sector Keys)

FPGA Sector
- Header Signature

Encryption Optional (Separate Sector Keys)

Quad ARM A53
- Header Signature

Encryption Optional
Summary and Next Steps

• FPGA or SoCs address multiple markets with different threat profiles

• Threat profiles addressed in FPGA or SoC designs are changing rapidly

• FPGA and SoC future architectures address newer IoT and data center profiles

• Take advantage of these new security features in your architectures
Intel PSG Anti-Tamper Security Symposium

- 7 November, 2016
- Hillsboro Oregon
- Non-disclosure agreement (NDA) required
Additional Sources of Information

A PDF of this presentation is available from our Technical Session Catalog: www.intel.com/idfsessionsSF.