Hardware Root-of-Trust for Cyber Security

Mark M. Tehranipoor
Intel Charles E. Young Endowed Chair Professor in Cybersecurity
Director, Florida Institute for Cybersecurity Research
Electrical and Computer Engineering Department
Example Hardware Attacks

- Trojans
- Untrusted Foundry
- Counterfeit ICs
- Physical Attack
- Side-channel
- Fault Injection
- Reverse Engineering
- Fake Parts
The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

October 4, 2018
SoC Security is a Challenge

- Tens of billions of transistors
- Custom/legacy functionality
- Many security critical assets
- Designed around the globe
- Tens of IPs from 3P vendors
- Aggressive time-to-market
Possible Attacks

### Existing Security Threats

- **Hardware Trojans**
  - Malicious modification of design by adversaries
  - Inserted by rogue employees of design house or foundry
  - Intentionally introduced → Denial of Service, information leakage

- **Side Channel**
  - No modification of design
  - Extraction of secret information through communication channels of ICs

- **Information Leakage**
  - Created intentionally by 3PIP vendor or induced unintentionally by CAD tools
  - Reveal of information to unauthorized parties

- **Fault Injection**
  - Power/Clock glitch, temperature variation, light/leaser/EM injection by malicious intention
  - Violation of confidentiality, integrity, and etc.

### Exploitation of Test/Debug Infrastructure

- Scan, Compression, JTAG etc.
- Exploitation of controllability and observability of a design maliciously
Security along SoC Design Life-cycle

Specifying | Planning | Alg/Arch. | Integration (RTL→Layout) | Tape-out / Silicon | Production

Pre-Silicon

Risk/Security Assessment

Secure Architecture
Threat Modeling;
Define architecture support for security;
Review architecture level security Policies

Pre-silicon Security Verification:
Threat Modeling; Design review; Security verification against attacks at different stages of the design process;

Post-Silicon

Risk/Security Assessment
Includes definition of assets, threat model, adversaries, and security policies

Security Arch. & Policies

Security Validation

Post-Silicon Security Verification:
Fuzzy test, Negative test, and penetration test
Security along SoC Design Life-cycle

Pre-Silicon

Register Transfer Level

Gate Level Netlist

Physical Layout

Post-Silicon

3PIPs

RTL

Synthesis

DFT/DFD Insertion

Netlist

Physical Design

Layout

GDSII Fab

Risk/Security Assessment

Security Arch. & Policies

Security Validation

Security Validation

Security Validation
Understand Supply Chain Vulnerabilities

- IP Piracy, Untrusted IP Vendor, CAD Tools, system integration
- Overproduction Out-of-Spec/Defective Tampering
- End of Life/Recycling

Maximum Flexibility

- Design
- Fabrication
- Assembly
- Distribution
- Lifetime

Minimum Flexibility

- Specification
- RTL
- Gate-level Netlist
- Layout
- GDSII
- Mask
- Fabrication (wafer)
- Wafer sort
- Dicing Wafer
- packaging
- Test
- To Market
- Distributors
- Orders
- System Integration
- System's end of life
- Recycling
- To Market

All Countereft Types, Tampering, SCA, Reverse Eng.
Solutions, with Lifecycle in Mind

Protect the IP

Protect the Assets

Protect the Supply Chain

- SoC Design
- SoC Integrator
- Foundry
- Packaging & Distribution
- End-user
Protect IP
Logic Locking or Obfuscation

- **Runs of Key gates-**
  - keys gates connected back-to-back
  - K1, K2 forms a run that can be replaced by K3

- **Dominating Key gates-**
  - K2 lies on every path from K1 to outputs
  - K2 is dominating key gate whose bit value can only be determined after muting K1

- **Mutable convergent Key gates-**
  - K1 & K2 converges at some other gate, such that K1’s bit value can be determined by muting K2 and vice versa
Protect IP, Against Piracy

Logic Locking

- Inserting key gates to lock the design and functionality of the chip
- Writing the correct key in a tamper-proof non-volatile memory on the chip after fabrication to unlock the functionality of chip
A number of vulnerabilities must be addressed to make logic locking a viable technology.
Defense-in-Depth

To defend a system against any particular attack using several independent methods
Defense-in-Depth for Protecting Obfuscation

Protect Against Malicious Change

Optical (Contactless) Attacks

FIB/Probing Attacks

Scan Attacks

Functional Locking Attacks

Key

L1 L2 L3 L4 L5 L5 L4 L3 L2 L1
Layer 1: Trojan Scanner

- Outer package removal.
- Chemical de-capsulation
- Backside thinning ~ 0um

Setting Parameters
i. High Voltage (HV)
ii. Dwelling time (Speed)
iii. Field of View (FoV) / (Magnification)
iv. Resolution

Capturing Images
(a) IC Under Auth. (IUA)

Image Registration
- Noise Removal - FFT BP filter
- Binarization - Adaptive Thresholding
- Smoothening - Gaussian Filter
- Flood Fill

Detection
- Optimized - Structural SIMilarity Index (SSIM) algorithm.
- Threshold based image labelling of suspicious areas of chip.
Protect Assets
Asset: A resource of value worth protecting from an adversary

Security Assets in SoCs:
- On-device keys (developer/OEM)
- Device configuration
- Manufacturer Firmware
- Application software
- On-device sensitive data
- Communication credentials
- Random number or entropy
- E-fuse,
- PUF, and more…

Source: Intel
Protect Assets: Strong Algorithms, Weak Implementation

- **Strong Algorithm & Architecture**
- **Weak Implementation & Execution**

Algorithms, architectures, and policies could be impacted by design methods that do not understand Security!

**Vulnerabilities**
- Information Leakage
- Side Channel Leakage
- Fault Injection
- IP Tampering, Trojan Insertion

**Accesses/attack surfaces**
- Remote Access (E.g., WiFi, Ethernet, Zigbee, etc.)
- PCB Access (E.g., JTAG and Debug ports)
- Physical Access
Gate Level -- Information Leakage

- Modeling an asset as **a stuck at fault**
- Utilize automatic test pattern generation algorithms to detect that fault
- A **successful** detection → Existence of information flow

We need to identify all observe points → Asset can be observed
Confidentiality Analysis

<table>
<thead>
<tr>
<th>Encryption Algorithm</th>
<th>Design</th>
<th>Seq. Elements</th>
<th>Observable Points</th>
<th>Distance</th>
<th>Stimulus</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Min</td>
<td>Max</td>
</tr>
<tr>
<td>AES</td>
<td>high speed</td>
<td>10769</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>small area</td>
<td>2575</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>ultra-high speed</td>
<td>6720</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Single-DES</td>
<td>small area</td>
<td>64</td>
<td>32</td>
<td>11</td>
<td>15</td>
</tr>
<tr>
<td>Triple-DES</td>
<td>small area</td>
<td>128</td>
<td>48</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>high speed</td>
<td>8808</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>RSA</td>
<td>basic</td>
<td>555</td>
<td>32</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>PRESENT</td>
<td>light ware</td>
<td>149</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

**Takeaways**

- All implementation of AES, RSA and PRESENT encryption modules have vulnerability due to DFT insertion.
- The ‘Distance’ and ‘Stimulus’ → quantitative measure of vulnerability.
- Higher value → less vulnerable.
Power Side Channel Attacks
Block Leakage Analysis
Security Rule Check

1. Establishing Secure Design Infrastructure

2. Development of Security Rules and Metrics

3. Development of Security-aware Automated CAD Tools

4. Experimental Security Validation
Objective: Provide automated security assessment and possible countermeasures of given designs for target vulnerabilities

Outcomes: Comprehensive set of formally defined transaction rules with security guarantees and data protection
Chip Backside Is A New Backdoor

- **Frontside**: Multiple interconnect layers obstruct the optical path to transistor devices
- **Backside**: Active devices are directly accessible
  - Photon Emission
  - Laser Stimulation/Fault Injection
  - Optical Contactless Probing

Source: C. Boit et. al.
Attacking Bitstream Encryption of FPGAs

- Device under Test (DUT): Xilinx Kintex 7 development board
  - Chip’s technology: 28 nm
  - No chip preparation (e.g., depackaging, silicon polishing, etc.)
- Optical Setup: Hamamatsu PHEMOS-1000
  - Laser wavelength: 1.3 \( \mu \)m
  - Laser spot size: >1 \( \mu \)m

- Non-destructive
- Non-invasive
- No Footprint
Localizing the Configuration Logic

Xilinx Kintex 7 in flip-chip package

Image acquisition with a infra-red laser scanning microscope

Localizing the Configuration Logic

Random Logic
Localizing Decryption Core using EOFM

Clock activity for unencrypted bitstream
Localizing Decryption Core using EOFM

Clock activity for encrypted bitstream
Locating the plaintext data

Locations in AES output port
Key Extraction

- Protection
  - Circuit Level Solutions
  - Device Level solutions
  - Material Level Solutions

NVM

Encrypted bitstream: 10111001010

AES Decryptor

Bitstream: 010101...

OBIRCH (TLS)

key = 0xd781b86f274630b561f39c9736f512eb0adf714f0d5c836c7a76ff627aca4923
Protect the Supply Chain
OCM: Enrollment & Ownership Release

1. Enrollment request
2. (2)/(5) Mutual verification
3. Ready to receive
4. Enroll chip information
5. Enrollment result
6. Ownership release request
7. Ownership release certificate

<table>
<thead>
<tr>
<th>Marking</th>
<th>ECID</th>
<th>CRPs</th>
<th>PID</th>
<th>SID</th>
<th>Trans. time</th>
<th>Stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM952A</td>
<td>0000</td>
<td>0158</td>
<td>2AB3</td>
<td>9EAF</td>
<td>null</td>
<td>null</td>
</tr>
<tr>
<td>CCLAL5902VLA</td>
<td>0000</td>
<td>0158</td>
<td>2AB3</td>
<td>9EAF</td>
<td>Jun/03/2017/11:30:21AM</td>
<td>IP owner/Fab</td>
</tr>
</tbody>
</table>

Counterfeit detection sensor embedded
IP owner/Fab
AutoBoM: External Visual Inspection of PCB

Smart phone w/ adapter

Image Pre-processing

Bill of Material
- Chips
- Resistors
- Capacitors
- Ports

Analysis and Defect Recognition
- Chips
- Discrete Components
- Solder
- Contacts
- PCB

Intelligent Microscopy for even lower time/cost!

Optical Microscopy
Auto3D: Internal Inspection of PCB

X-ray CT
- Parameter Optimization
- Sample Preparation and Filtering

Image Processing and Segmentation
- Separate Layers
- Traces
- Vias w/ Pads
- Vias w/ Anti-Pads
- Conductive Planes

CAD File Generation
- Vectorization
- PCB CAD File (PCB, DWG, DXF, etc.)

PCB Analysis
- Trace timing
- Signal integrity
- Power integrity
- Electromagnetic Interference
- Thermal Footprint
- Security vulnerabilities

Nondestructive!
Non-destructive Reverse Engineering
SCAN Lab at FICS Research Institute

Florida Institute for Cybersecurity (FICS) Research
Recommendations

• **Designed-in security**
  • Standards: Logic Locking, SCA, Backside, Provenance, Traceability

• **Automation**
  • Reduce complexity & cost

• **Design with life cycle in mind**
  • Device → Systems
  • Traceability & provenance
Recommendations

• Powerful but low cost inspection

• Hardware upgrade → Zero day

• Smart devices → DT for secure semiconductors