2007

Security Primitives for Reconfigurable Hardware [presentation]

Huffmire, Ted

Ted Huffmire. Security Primitives for Reconfigurable Hardware. Faculty Candidate Seminar, Department of Computer Science, Room GE-117, Naval Postgraduate School, Monterey, CA,
Threats and Challenges in FPGA Security

Ted Huffmire
Naval Postgraduate School
December 10, 2008
## Overview

<table>
<thead>
<tr>
<th>Problem Areas</th>
<th>Foundry Trust</th>
<th>Physical Attacks</th>
<th>Design Tools</th>
<th>Design Theft</th>
<th>System Assurance</th>
</tr>
</thead>
</table>

### Attacks

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Trojan horse</th>
<th>Backdoor</th>
<th>Kill switch</th>
<th>Probing</th>
<th>Sand and Scan</th>
<th>Side Channels</th>
<th>Data Remanence</th>
<th>Covert channels</th>
<th>Side channels</th>
<th>Bypass</th>
<th>Cloning</th>
<th>Reverse engineer</th>
<th>Readback attack</th>
<th>DoS Authentication</th>
<th>Complex designs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Solutions

<table>
<thead>
<tr>
<th>Solutions</th>
<th>Trusted foundries</th>
<th>FPGAs</th>
<th>X-Ray Inspection</th>
<th>Sand and Scan</th>
<th>Tamper sensing</th>
<th>Adding noise</th>
<th>Degaussing</th>
<th>Logical isolation</th>
<th>Tracing wires</th>
<th>Sanitization</th>
<th>Continuous power</th>
<th>Encrypt bitstream</th>
<th>Watermarking</th>
<th>Authentication</th>
<th>Reference monitor</th>
<th>Defense in depth</th>
<th>User training</th>
<th>Security usability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Future Research

<table>
<thead>
<tr>
<th>Future Research</th>
<th>All of supply chain</th>
<th>Lessons from S/W</th>
<th>Red teams</th>
<th>Side channels</th>
<th>Trusted tools</th>
<th>Verification Languages</th>
<th>CM</th>
<th>High-assurance Partial reconfig PUFs</th>
<th>High-assurance CMPs</th>
<th>Tagging</th>
<th>Dynamic security</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Note: The table structure and content are designed to provide a structured overview of the topics discussed in the document, including problem areas, types of attacks, solutions, and future research directions within the context of foundry trust and physical attacks.
Reconfigurable Hardware

FPGA Chip

SDRAM (off-chip)

Reference Monitor

AES

CPU Core

Crypto Core

CPU Core
Protection Alternatives

Separate Processors

Reconfigurable Protection

Separation Kernels

Physical

Spatial

Software

Temporal
Design Flows

Flowchart illustrating the design process for FPGA chips, including:

- **MATLAB Algorithms**
  - HDL Synthesis
  - Logic Synthesis
  - Place and Route
  - Bitstream

- **Accel DSP**
  - HDL Synthesis
  - Logic Synthesis
  - Place and Route
  - Bitstream

- **C Code**
  - Celoxica
  - Soft Core

- **C Code**
  - gcc
  - Executable

- **FPGA Chip**
  - SRAM Block
  - Soft DSP Core
  - Soft AES Core
  - Hard Core

- **DRAM** (off-chip)
  - DRAM
Intertwined Cores

Core A and B significantly overlapping

long interconnects

switchbox

one set of logic blocks and associated routing

small FPGA design with 2 cores
Moats

SDRAM (off-chip)

Reference Monitor

AES

Crypto Core

CPU Core

FPGA Chip
Moats 1.0
Moats and Drawbridges

- Core 1
- Core 2
- Core 3
- Core 4

□ = IOB  □ = Moat CLB  □ = Core CLB
Interconnect Tracing

SDRAM (off-chip)
Communication Architecture

FPGA Chip

SDRAM (off-chip)

Arbiter/Reference Monitor

CPU Core

Crypto Core

AES

CPU Core
Memory Protection

- FPGA Chip
- DRAM
- DRAM
- DRAM
- DRAM
- SDRAM (off-chip)
- Crypto Core
- AES
- CPU Core
- Reference Monitor
- X
1. Policy
Access->\{Module1, rw, Range1\} \\
| \{Module2, rw, Range2\}; \\
Policy->(Access)*;

2. Build Parse Tree

3. Transform Parse Tree

4. Regular Expression
\(({\{\text{Module1, rw, Range1}\}} \\
| \{\text{Module2, rw, Range2}\})^*\)

5. NFA

6. DFA

7. Verilog

8. Reference Monitor
SoC Application

On-Chip Peripheral Bus (OPB)

µBlaze0

µBlaze1

RS232

DDR SDRAM

AES

Ethernet

Authentication Module

To Network
Questions?

- http://faculty.nps.edu/tdhuffmi