Exploitable Bugs in Hardware Designs

Cynthia Sturton

2017 SaTC PI Meeting
Breakout Session

Outline

- Vulnerable vs. malicious hardware: an orthogonal problem
- Security vulnerabilities do exist
- New opportunities for the attacker
- Research questions

Malicious Hardware

- Threats
  - Malicious foundry
  - Malicious design
- Risks
  - Backdoor
  - Degrade quality
  - Reduce lifespan
  - Weaken cryptographic primitives

Vulnerable Hardware

- We found roughly 9% of recent, published AMD errata were security critical [ASPLOS 2015]
- Of 185 patches and bug reports for OR1200, we found 25 to concern security critical bugs [ASPLOS 2017]
- Intel SYSRET issue
  - Not a bug, but still a vulnerability
- Password protected JTAG functionality

New Opportunities for the Attacker

- A move toward open source
  - RISC-V
- IoT
  - Number of chips extant in the world
  - Cheap devices → Tight budgets → Security given short shrift

Promising Directions and Open Questions

- Verification for security
  - What are the properties we should be verifying?
- Static analysis of hardware designs
  - What are common patterns (e.g., in RTL) that lead to security vulnerabilities?
- Understanding which vulnerabilities lead to security risks
  - Can we automate the process of finding exploits if they exist?
- Dynamic verification for detection of vulnerabilities
  - Can we make it practical to use dynamic verification in the field?
  - Can we drive dynamic verification toward the detection of security bugs?

Open Question

- Can we evaluate the extent of the problem?