

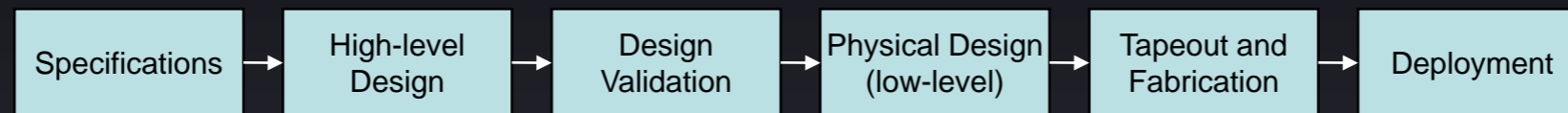
Race to the bottom: Malicious Hardware

Angelos D. Keromytis

(joint work with Simha Sethumadhavan and Ken Shepard)

Columbia University, USA

Modern Hardware Manufacturing



- Outsourced manufacturing
- Extensive IP component integration
 - IP from different vendors/sources
- Consolidation of fabrication
 - 59 facilities world-wide that can produce 300mm wafers [Source: US DoD]

- Malicious functionality inserted into hardware during design, integration, or manufacturing
Hardware Easter Eggs (HEEs)
- also possible during equipment servicing
- practically impossible to detect or mitigate
 - hardware is assumed trusted
- Variety of triggers: time, data, other external signal
- Can attack confidentiality, integrity, availability

Technical Feasibility

- IBM demonstrated low-gate-count key-leakage HEE
- Upcoming paper in LEET shows generic “malicious processor” embedded in CPU in under 2K gates!
 - much more powerful software-hardware combined attacks
- Updatable microcode vulnerabilities

Injection Feasibility

- Variety of ways to inject HFE



- malicious/disgruntled/bribed employee at variety of locations (design, integrate, fab, service)
- can even imagine remote compromise of designer's system
- Attacker must be motivated or have easy access
- Risk of capture/detection/attribution is very low

Modified Steilmeier Questions (1)

- governments, military, intelligence, public safety, high-value IT-intensive industries
- What is done/can be done today?
 - trusted source (who?!)
 - testing (limited capabilities)
 - diversity of sources (only 59 fabs @ 300mm...)
 - reverse engineer (~1 week and \$250K per chip)⁶

Modified Heilmeier Questions (2)

- What needs to be done?
 - concerted, multi-thrust research effort
 - architecture support (combined hardware/software solutions) needed
 - possible directions:
 - secure design & analysis/testing,
 - runtime detection & validation (side-channel analysis, BFT, emulation, microcode ISR)
 - software-controlled hardware

Modified Heilmeier Questions (3)

- Why do I think it can be done?
 - significant advances in theory and practice in design, analysis (of various types)
- What are the risks and payoffs?
 - if not done: vulnerable IT/computing infrastructure at the lowest possible level
 - if successful: establish trust in said infrastructure

Modified Heilmeier Questions (4)

How much will it cost? How long will it take?

- 3-5 year effort, need to cover space of possible solutions (sorry, no \$\$\$ figure)
- How do we measure success (midterm/final)?
- metrics appropriate to each class of techniques (prevention, mitigation, detection)
- red team testing against sample