FPGA-based Systems -- Vulnerabilities and Countermeasures

Cybersecurity Specialization
-- Hardware Security

Vulnerabilities in FPGA Systems

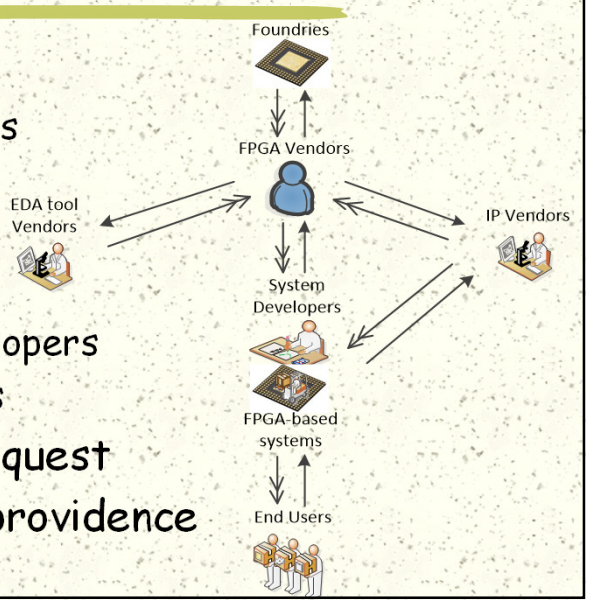
- Side channel attacks
  - Power analysis
  - Timing analysis
  - Electromagnetic emanation analysis
- Fault injection attacks
  - Glitch analysis
  - Ionizing radiation analysis
- Physical attacks
  - SRAM FPGAs
  - Anti-fuse FPGAs
  - Flash FPGAs

Vulnerabilities in FPGA Design

- HDL level
  - Who: designer, third party IP
  - How: steal design IP, insert Trojan into design
- Synthesis level
  - Who: designer, EDA tools
  - How: illegal use of EDA tools, Trojan insertion, design IP piracy
- Bitstream level
  - Who: user
  - How: IP misuse

Supply and Demand Model

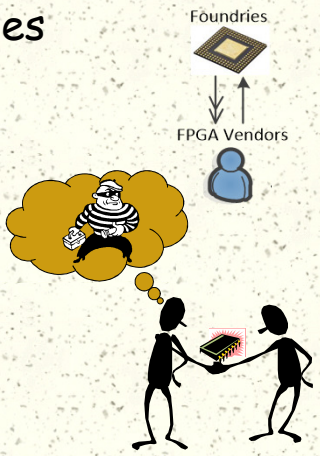
- Six parties
  - FPGA vendors
  - foundries
  - IP vendors
  - tool vendors
  - system developers
  - system users
- →: service request
- -->>: service providence



Vulnerabilities and Attacks (I)

FPGA vendors vs. foundries

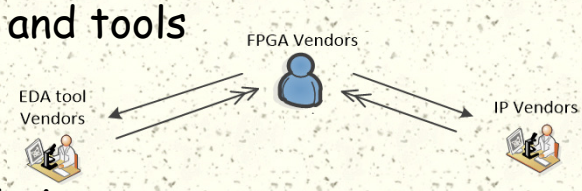
- Request: fabrication
- Service: FPGA chips
- Threats
  - Overbuilding
  - Hardware Trojan
  - Information leaking



Vulnerabilities and Attacks (II)

FPGA vendors vs. IP/EDA tool vendors

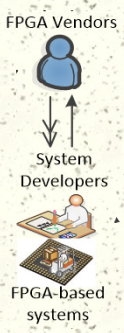
- Request: IPs and tools
- Service:
- Threats
  - Hardware Trojan
  - Information leaking
    - IP protection
    - Reverse engineering



Vulnerabilities and Attacks (III)

System developers vs. FPGA vendors

- Request: FPGA chips
- Service:
- Threats
  - Hardware Trojan
  - Information leaking



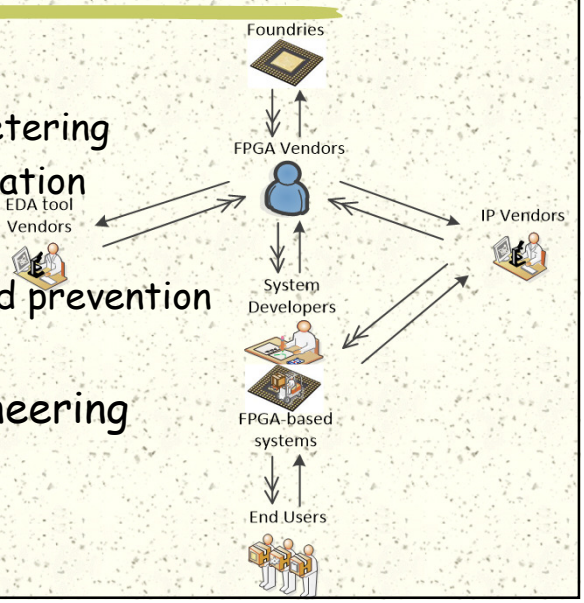
Vulnerabilities and Attacks (IV)

End users vs. system developers

- Request: system
- Service:
- Threats
  - Hardware Trojan
  - Information leaking
    - Cloning/reverse engineering
    - Side channel attacks
    - FPGA replay attack

State-of-the-Art Defenses

- Overbuilding
  - Hardware metering
  - Remote activation
- Trojan
  - Detection and prevention
  - Testing
- Reverse engineering
  - Encryption
  - Obfuscation



State-of-the-Art Defenses

- Cloning
  - Watermarking
  - Fingerprinting
  - Binding with encryption and PUF
- Side channel attacks
  - Methods proposed for passive attacks
- FPGA replay attacks
  - Remote update protocol
  - Reconfigurable binding