SAFE: SECURITY AUTOMATION FOR FABRICATED ELECTRONICS

SHAWN BLANTON
ECE DEPT.
CARNEGIE MELLON
PITTSBURGH, PA USA
SEPTEMBER 25, 2019
Software security, what comes to mind?

**Threats**
- Malware
- Backdoors
- Viruses
- Worms
- Ransomware
- Trojans
- Key loggers
- Spyware
- Denial of Service

**Defenses**
- Root of Trust
- Gateway
- Antivirus
- Firewall
- Passwords
- Authentication
- VPNs
- Access control
- Encryption
Hardware security, what comes to mind?

**THREATS**
- Trojans
- Counterfeiting
- IP Piracy
- Supply Chain
- Side channels
- Overproduction
- Reverse Engineering
- Recycling

**DEFENSES**
- Logic Locking
- Split Chip
- Split Fabrication
- Passwords
- Watermarking
- Monitoring
- Obfuscation
- Access control
- CRYPTOLOGIC
Is Hardware Security Real?

The Hunt for the Kill Switch

Are chip makers building electronic trapdoors in key military hardware? The Pentagon is making its biggest effort yet to find out

By Sally Adee

Last September, Israeli jets bombed a suspected nuclear installation in northeastern Syria. Among the many mysteries still surrounding that strike was the failure of a Syrian radar—supposedly state-of-the-art—to warn the Syrian

Trojans aren’t restricted to the software domain

Trojans aren’t restricted to the software domain; in some instances, hardware Trojans could even open backdoors in custom silicon. Outsourcing has reshaped the way electronics products are made—and helped to cut manufacturing costs massively. But, as production margins have fallen, so too has trust in the organisations that make up the supply chain. Companies which rely on outsourced manufacturing are having to come

DARPA Announces Next Phase of Electronics Resurgence Initiative

Expanded program portfolio seeks to increase access to DoD-specific electronics manufacturing capabilities, enhance hardware security, and ensure ERI investments translate to DoD applications

OUTREACH@DARPA.MIL
11/1/2018

What’s All This Mislabeled IC Stuff, Anyhow?

Buyer beware when purchasing chips from non-top-tier suppliers—be sure you’re getting the real deal, otherwise reverse-engineering your designs (or worse) likely awaits.

Paul Rako | Oct 04, 2017

Orange County Distributor Charged With Selling Counterfeit ICs

May 3, 2018 | 1 Comment | News Analysis | By Barbara Jorgensen
Why is **Hardware** Security Needed?
Integrated Circuit Design, Fab & Test

Side channels

Trojans

IP Piracy

Supply Chain

Recycling

Overproduction

Reverse Engineering

Integrated Circuit Design

RTL

Logic Synthesis

Netlist

Physical Synthesis

Layout

Chip

Test & Assembly

Wafer

IC Fabrication

IP vendor

synopsys

ARM

Integrated
circuit
design

Integration
team

In-house

IP

vendor

reverse engineering

trojans

overproduction

supply chain

counterfeiting

IP piracy

recycling
Logic Locking [Roy, Computer 2010]

**Idea:** *Use a secret key to mitigate illegitimate use, attacks,...*

- Extra (key) inputs are used to invert circuit signals
- Key is stored in a tamper-proof memory

**Challenges:** Overhead, lock strength, etc.

![Diagram of protected netlist with secured memory and key bits](attachment:protected_netlist_diagram.png)
Logic Locking
Arms Race

LOCKING SCHEMES
- Logic Locking
  Roy, Computer 2010
- Strong Logic Locking
  Roy, Computer 2012
- Fault-based Locking
  Rajendran, DATE 2012
- SARLock
  Yasin HOST 2016
- AntiSAT
  Xie, ICCCHES, 2016
- TTLock
  GLSVLSI 2017
- Signal Probability Attack
  Yasin, ASP-DAC 2017
- SFLL
  Yasin, ACM CCS 2017

LOCKING ATTACKS
- ATPG Attack
  Roy, Computer 2012
- SAT Attack
  Subramanyan, HOST 2015
- Signal Probability Attack
  Yasin, ASP-DAC 2017
- Removal Attack
  Yasin, IEEE TETC 2018
- CLIC-A, Duvalsaint
  ITC-ASIA 2019, ITC 2019

SAT Attack Resilient Logic Locking

Inputs → Original circuit → Mask
Input == Keys
Keys

Circuit Diagram:
- Original circuit
- Input == Keys
- Mask