Secure Hardware in the Nano Era: Some New Directions

Swarup Bhunia
T. and A. Schroeder Associate Professor
Electrical Engineering and Computer Science

SoC Security Issues & Protection

IP-based Design Flow
- IP Vendor
  - Hardware IP
- IC Design House
  - GDS-II
  - Fab
    - Reverse-engineer GDS-II
    - Manufacture illegal IC instances
  - Make illegal copies of the IP
    - (avoid paying royalty)
    - Modify IP and sell under different brand-name
- Deployment
  - Insert Trojans
  - Make clones
  - Leak secret information

Security Threats
- Insert hardware Trojan in IP
- Make illegal copies of the IP
- Modify IP and sell under different brand-name
- Manufacture illegal IC instances
- Reverse-engineer GDS-II
- Insert Trojans
- Make clones
- Leak secret information

D-f-S Solutions
- Trojan-resistant design; improved detectability*
- Hardware Obfuscation#; Protect IP Eval. Copy*, PUF$
- SCA resistant Design**; Prevent scan-based attack***

*Wang et al., DFT, 2012; Narasimhan et al., Tcomp 2012, Chakraborty et al., CHES 2009; Narasimhan et al., D&T, 2012
**Wang et al., DAC 2013, Chakraborty et al. ICCAD 2008
Protection against IP Piracy: Hardware Obfuscation

- Primarily protects the IP owner!

What are the challenges?

Taxonomy of hardware IP security issues

Hardware Trojan Attacks!
Security Through Obfuscation

Basic Idea:

- Obfuscate the design functionally and structurally
- Achieved by modifying the state transition function
- Normal behavior is enabled only upon application of a key!

Prevents illegal usage of IPs!

Chakraborty & Bhunia, TCAD 2009

Results: Trojan Detectability

21% average improvement in Trojan coverage

Overhead:

- ~11% area, 11% power overhead at iso-delay
- Average run-time: ~1200 seconds (90% of total run-time taken by Tetramax)

Chakraborty & Bhunia, ICCAD 2009
From the SoC designer’s perspective, integrity of 3rd Party IPs need to be checked!

SoC Design House
IP Trust Validation
SoC Integration
SoC Design Convergence

Foundry

Hardware IPs
CPU
Memory
Bus
DSP
Trojan
Backdoor

Anti-Counterfeiting Design Solutions
Threats & Vulnerabilities

• Globally distributed semiconductor business model
  - Ample *sneak paths* to insert counterfeit chips

  ![Semiconductor Business Model](image)

• Two Broad Categories:
  - *Recycled/Remarked*: selling of used/aged chips as new
  - *Cloned New Chips*: IP piracy, reverse-eng, overproduction

Examples of Physical Unclonable Functions (PUFs)

- **RO PUF**

- **Arbiter PUF**
  - Lee *et al.*, 2004

- **Butterfly PUF**
  - Kumar *et al.*, 2008

- **SRAM PUF**
  - Guajardo *et al.*, Holcomb *et al.*, 2007

*Can we generate “robust” “strong” PUF using on-chip structure?*
**PUFs Using On-Chip Structure**

MECCA PUF
- Krishna et al, CHES 2011

RESP PUF
- Zheng et al, DAC 2013

Scan PUF
- Zheng et al, ASP-DAC 2013

**Active Defense against IC Cloning**

- A chip locking approach with *antifuses (AF)* on I/O port
  - AF is an *OTP, normally open* switch\(^1\) (\(R_{\text{off}} \sim 100\text{M} \text{ -- } 1\text{G} \Omega\))
  - AF program on *correct key input* (stored in on-chip NVM)
  - *Active defense* against recycling/cloning

1. W. T. Li et al., EDL, 2000
2. N. Robson et al., CICC, 2007
Hardware Trojan Attacks: “A Problem from Hell*”

MIT Technology Review

NSA’s Own Hardware Backdoors May Still Be a “Problem from Hell”

Revelations that the NSA has compromised hardware for surveillance highlights the vulnerability of computer systems to such attacks.

By Tom Simonite on October 8, 2013

In 2001, General Michael Hayden, who had earlier been director of both the National Security Agency and the Central Intelligence Agency, described the idea of computer hardware with hidden “backdoors” planted by an enemy as “the problem from hell.” This month, news reports based on leaked documents said that the NSA itself has used that tactic, working with U.S. companies to insert secret backdoors into chips and other hardware to aid its surveillance efforts.

Michael Hayden

*Michael Hayden

HW Trojan Attacks: in the News

Fishy Chips: Spies Want to Hack-Proof Circuits

By Adam Reiswiger

In 2013, the U.S. military had a problem. It had bought more than 50,000 microchips designed to be secure from hacking by its supplier, a subsidiary of a Chinese firm. After Navy weapons systems, the chips could have been hacked, able to shut off a missile in the event of war or be used to collect data.

March ISQED 2015

The Navy Bought Fake Chinese Microchips That Could Have Disarmed U.S. Missiles

By Adam Reiswiger

The Navy bought more than 50,000 microchips for use in everything from missiles to computer servers, but all of them turned out to be counterfeit from China.

March ISQED 2015

Can DARPA Fix the Cybersecurity ‘Problem From Hell’?

By Adam Reiswiger

There are computer security threats — and there are computer security nightmares. Put subverted circuits firmly in the second category. Last week, retired Gen. Michael Hayden, the former CIA and NSA chief, called the breach of hacked hardware “the problem from hell.”
HW Trojan Threats

Most vulnerable stages!

Modern SoC Design and Manufacturing Flow*


HW Trojan Examples/Models

Comb Trojan Example

Seq Trojan Example

MOLES*: Info Leakage Trojan

Comb Trojan model

Seq. Trojan Model

System level view

*Lin et al, ICCAD 2009

March ISQED 2015
Introduction to Trojan Detection

- Taxonomy of Existing Trojan Detection Approaches

Side-channel approaches do not require triggering the Trojan to observe its impact at primary input nodes.

Methodology

- Multiple-parameter Approach for Trojan Detection

  - Due to process variations, it is extremely challenging to detect the Trojan by considering $F_{\text{max}}$ or $I_{DDT}$ individually.
Methodology

• Multiple-parameter Approach for Trojan Detection
  - Due to process variations, it is extremely challenging to detect the Trojan by considering $F_{\text{max}}$ or $I_{\text{DDT}}$ alone.

![Graph showing the relationship between $F_{\text{max}}$ and $I_{\text{DDT}}$.]

- Consider the intrinsic relationship between $I_{\text{DDT}}$ and $F_{\text{max}}$ together, $I_{\text{DDT}}$ vs. $F_{\text{max}}$

![Graph showing the relationship between $I_{\text{DDT}}$ and $F_{\text{max}}$.]

- c880 from ISCAS-85 benchmark suite with 8-bit ALU circuit Trojan
  - March ISQED 2015
Statistical Approach

- Feasible Trojan search space is inordinately large!
  - Exhaustive enumeration impossible
  - Deterministic test generation computationally infeasible

- A Statistical Approach for Trojan Detection
  - Finds the rare events in the circuit
  - Generates test vectors to trigger each trigger node multiple times ($N$ times)
  - Provides high confidence about detecting arbitrary Trojans!

Circuit Example

(i) Combinational Trojan
(ii) Sequential Trojan

- Trojan Trigger Condition:
  (i) $a=0$, $b=1$, $c=1$
  (ii) $a=1$, $b=0$

- Generate vectors to satisfy each of these conditions multiple ($N$) times
- Probability of Trojan activation increases with $N$
- The concept is similar to $N$-Detect Tests*

* I. Pomeranz and S.M. Reddy, 2004
**Self-Referencing: Golden-Free Trojan & Counterfeit Detection**

- Seq. ckts have diff. switching currents based on both input & state conditions
- Uncorrelated switching in time is attributed to a seq. Trojan!
- Seq. Trojans impose greater threats!

---

**Temporal Self-Referencing**

- DLX circuit w/o & w/ Trojan FSM

---

**No golden chip is required!!!**
Integrative Measures …

Design for Security → Trust Validation → Security Monitoring

Secure by design, test and run-time monitoring!


March ISQED 2015

Infrastructure IP for Security:
A Scalable Solution to SoC Security & Debug

Wang et al., IEEE Tcomp, To Appear

New SRC grant
Infrastructure IP for SoC Security (IIPS)

- **IIPS** is a *centralized* IP block for various security protections
- **Major Features of IIPS**
  1. *Ease of integration; plug-n-play using IEEE 1500 Standard*
  2. *Reusable IP*
  3. *Configurable*
  4. *Functionally scalable & flexible*
  5. *Minimal performance/power/area overhead*
  6. *Does not affect IP level design & IP integration in SoC*
  7. *Can be merged with other (e.g. test / debug) infrastructure IPs*

---

**Custom Design of IIPS**

- **Target threat models:** *scan-based attack, IP piracy, HT attacks …*
- **Mitigation strategies:** *scan chain authentication, ScanPUF, path delay based Trojan detection …*
- **IIPS** contains a *Master Finite State Machine (M-FSM), a scan chain enabling FSM (SE-FSM), and a clock control logic*
- **IIPS interface**
  - Inputs: standard SoC test inputs, an active low reset *IIPS_RSTN*
  - Outputs: a scan enable for each IP, test clock (*WRCK*) & test control signals (i.e. *ShiftWR*, *CaptureWR*)
- **Locking states SC_LOCK and TD_LOCK** designed to support scan chain based SoC testing and delay fault testing
ScanPUF Primitive

- Desired features of PUF in IIPS: low-overhead, IEEE 1500 compliant signature generation and extraction, test reusable via Core Test Language (CTL)
- As a case study, we choose the ultralow-overhead ScanPUF which exploits the existing scan chain DFT structures in an SoC

IIPS Test Protocol under IEEE Std. 1500

- The control of M-FSM and SE-FSM is at SoC level
- ScanPUF and HT detection test sets are developed at core level and expanded to SoC level
- Test procedure: (1) core test mode configuration; (2) test initialization; (3) signature gen.; (4) signature propagation
- Trojans in a core: LOC & LOS; Trojans on interconnects: LOS

Algorithm 1 SoC level test protocol for Trojan detection

Xiao et al. D&T 2013
Integrity Validation in Printed Circuit Boards (PCBs)

Security Attacks in PCB

• PCBs are increasingly vulnerable to Counterfeiting/Tampering attacks:
  - Long distributed supply chain
  - Global design/manufacturing team
  - Rapid rise of PCB design cost & complexity
  - Easier to hack/tamper
  - Makes *Trojan attacks viable*

- Ghosh et al., IEEE D&T, To Appear
- Provisional Patent

*Ghosh et al., IEEE D&T, To Appear*
Protecting PCBs against Counterfeiting

• PCBs go thru. long distributed supply chain
• PCBs can be authenticated by unique signature from each board
• Key ideas to generate unique signature for each PCB
  - Exploit variations in Cu Trace impedances
  - Generate unique signature from each PCB
  - Use existing test equipment's for integrity validation

Zhang et al., VTS 2015

Summary & Future Directions

• Protect all levels of hardware (IC, PCB, System)
• Integrative Solution – maximize confidence!
• Cost-Effectiveness – low design/test cost
• Easy to interface – with existing design tools & infrastructure!
• Explore new attacks/countermeasures for emerging devices – discover vulnerabilities & effective security solutions based on unique properties of post-CMOS devices!
Acknowledgements:

- Students in *Nanoscape Research Lab.*, Case
- Collaborators at Intel, IBM, UFL, GaTech, Purdue U., USF

Sponsors: