Understanding Integrated Circuit Security Threats

Asif Iqbal
Senior Program Manager, Apple Inc.
SDM '11
Outline

• Vulnerability at different layers and relative impact
• Some Cases and Proof of Concepts
• Integrated Circuit (IC) Design Flow
• Trust in IC development lifecycle
  – Stages of entry
  – Pre Silicon Attacks
  – In Silicon Attacks
  – Post Silicon Attacks
• Deep Dive on Hardware Trojans
  – Trojan Anatomy
  – Trojan Classification
  – Design Examples
  – Challenges in detection
• Current Security Initiatives
Layers of information processing
Attacks at different layers

- Social Engineering
- Malwares / Macros
- Viruses/ Trojans
- ??
Key Takeaway #1: Hardware is the root of trust; Even a small malicious modification can be devastating to system security.
Internet of things

• 10 billion Devices and counting
• Everything right from your computer to your phone to your microwave can be compromised without you ever knowing about it.
“September 2007, Israeli jets bombed a suspected nuclear installation in northeastern Syria. Among the many mysteries still surrounding that strike was the failure of Syrian radar, supposedly state of the art, to warn the Syrian military of the incoming assault. It wasn’t long before military and technology bloggers concluded that this was an incident of electronic warfare and not just any kind. Post after post speculated that the commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden “backdoor” inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips’ function and temporarily blocked the radar”

Source: IEEE spectrum, 2007
Counterfeit Chips in Military

http://www.youtube.com/watch?v=H5z5F7SQvX0
A hidden 'back door' in a computer chip could allow cyber-criminals a way to override and control computer systems on Boeing 787s.

-- dailymail.co.uk, 30th May 2012

Laptop Batteries Can Be Bricked

• The method involves accessing and sending instructions to the chip housed on smart batteries
• completely disables the batteries on laptops, making them permanently unusable,
• perform a number of other unintended actions like false reporting of battery levels, temperature etc.
• could also be used for more malicious purposes down the road.
More Cases

Dell warns of hardware Trojan

Computer maker Dell is warning that some of its server motherboards have been delivered to customers carrying an unwanted extra: computer malware. It could be confirmation that the “hardware Trojans” ... are indeed a real threat.

- Homeland Security News Wire July 2010

F.B.I. Says the Military Had Bogus Computer Gear

...the .. sinister specter of an electronic Trojan horse, lurking in the circuitry of a computer or a network router and allowing attackers clandestine access or control, was raised .. by the FBI and the Pentagon. The new law enforcement and national security concerns were prompted by Operation CISCO Raider, which has led to 15 criminal cases involving counterfeit products bought in part by military agencies, military contractors and electric power companies in the United States.

Intel Ivy Bridge Can’t Keep Your Secret

• Sabotage on the cryptographic capability of Intel processors including the latest Ivy Bridge which is the heart of most 2012 PCs.
• Reduces the entropy of the random number generator from 128 bits to 32 bits.
• Accomplished by changing the doping polarity of a few transistors.
• Undetectable by built in self tests and physical inspection.

[Stealthy Dopant-Level Hardware Trojans, Georg T. Becker, Francesco Regazzoni, Christof Paar, and Wayne P. Burleson]
Key Takeaway #2: Virtually any and every electronic system around us can be potentially be compromised.
Semiconductor Economics

Moore’s Law
Capital Costs for setting up a foundry
Typical Useful lifetime of a foundry
Selling Price of a Chip
Gross Margins
Semiconductor Economics

- Moore’s Law and the market requirements for higher performance chips are driving the production of smaller transistors
  - Smaller devices and larger wafers
- Technology Changes every ~1.5 years
- Cost of Setting up a foundry ~$5-$10 Billion
  - Low yields for first few months
  - 6-9 months Learning curve in for process improvement.
- Cyclic demand for consumer electronic products
- Gross Margins less than 45% is not competitive if you do not have scale.
Impact on Semiconductor Product Design

• Time to Market Pressure
• Lots of Reuse
  – Third Party IPs – Sometimes cheaper than developing on their own
  – Third party tools and scripts
• Outsourced Manufacturing (Fab-Less Model)
• Outsourced Testing

Key Takeaway #3: Most semiconductor companies outsource their manufacturing due to the high capital and operational costs.
Security Implications of Outsourced Manufacturing

• Compromising the IC supply chain for sensitive commercial and defense applications becomes easy.

• Attacker could substitute Trojan ICs for genuine ICs during the process.

• Attacker could subvert the fabrication process itself by implanting additional Trojan circuitry into the IC mask.

• Fragmentation makes it easy for the counterfeit / recycled ICs to enter the supply chain.
IC Design Flow

- Lots of Third party IP and Code Reuse
- Complicated Scripts, Third Party tools
- Physical Placement of Gates, Heavy use of tcl scripts

Flow:
1. Requirements
2. Design Specification
3. RTL Coding
4. Functional Verification
5. Logic Synthesis
6. Gate Level Simulation
7. Place and Route
8. Layout Verification
Different Views of a Design

RTL:
```verilog
always @(posedge clock) begin : COUNTER // Block Name
    // At every rising edge of clock:
    if (reset == 1'b1) begin
        counter_out <= #1 4'b0;
    end
    // If enable is active, then:
    else if (enable == 1'b1) begin
        counter_out <= #1 counter_out + 1;
    end
end // End of Block COUNTER
```

NETLIST:
```
G D
Q O
```

GDSII:
Semiconductor Manufacturing Process

Semiconductor device fabrication is a series of four types of processing steps: deposition, etching, patterning, and modification of electrical properties. Additional measurement/metrology steps are added.

**Deposition**
Growing/transfering material onto wafer, wafer coating.
E.g. Wafers are put into a copper sulphate solution, and copper ions are deposited onto the transistor through a process called electroplating.

**Etching**
Removing material from the wafer either in bulk or selectively process used between levels.
E.g. Chemical Mechanical Planarization (CMP)

**Lithography**
Patterning and shaping of wafer materials
E.g. Wafer costing with a photo-resist that gets exposed by a stepper, a machine that focuses, aligns, and moves the mask exposing select portions of the wafer to short wavelength light.

**Electrical Property Modification**
Doping transistor sources and drains by diffusion furnaces and by ion implantation
Activating implanted dopants through Furnace or Rapid Thermal Anneal (RTA)

Trust in IC development Life Cycle
Key Takeaway #4: The trust in the chip design process is broken
Pre Silicon Attacks (Design Stage)

• Modification of Functional Logic
  – Third party corrupt IPs
  – Tampering with clocks
  – Tampering the voltage control logic

• Modification of Test and Debug Logic
  – Testability
  – Debug Logic
  – Vendor Controls

• Modification of the Layout
  – Thinning of the conducting wires
  – Weakening the transistors
  – Using Spare gates
In Silicon Attacks (Manufacturing Stage)

- Lithography processes present opportunities to print additional circuitry and devices
- Need to replace glass masks
  Masks are automatically loaded into litho tools
  No physical access to target tool required
- Other process and measurement/metrology steps present opportunities for causing scraps
- Trojan circuitry may be inserted in different layers of circuitry within the chip
- Long manufacturing lines (~200 processing steps)
  Many opportunities for malicious insiders
- Targeting processes at the BEOL (Back End Of the Line) causes higher damages to the IC manufacturer.
Different types of In Silicon Attacks

- **FAKE Counterfeiting** has become a big problem for the U.S. military, and bogus packaging could disguise a questionable chip as a legitimate one. **& BAKE** Baking a chip for 24 hours after fabrication could shorten its life span from 15 years to a scant 6 months.

- **NICK THE WIRE** A notch in a few interconnects would be almost impossible to detect but would cause eventual mechanical failure as the wire became overloaded.

- **ADD EXTRA TRANSISTORS** Adding just 1000 extra transistors during either the design or the fabrication process could create a kill switch or a trapdoor. Extra transistors could enable access for a hidden code that shuts off all or part of the chip.

- **ADD OR RECONNECT WIRING** During the layout process, new circuit traces and wiring can be added to the circuit. A skilled engineer familiar with the chip’s blueprints could reconnect the wires that connect transistors, adding gates and hooking them up using a process called circuit editing.

Post Silicon Attacks

- Modify Operating Conditions
  - Temperature
  - Power
  - Frequency
- FIBbing to cut or create connections
- Exploiting inbuilt security holes due to poor design
  - Invalid instructions
  - Protocol errors
  - Denial of service
- “Creative” Use of Test and Debug Modes and “Designer’s Backdoors”
The designers Backdoor!

Commonly built into chips by designers to allow quick and easy access to some test and debugging features:

- Can Allow cyber-criminals a way to override and control computer systems on Boeing 787s
- Security researchers have previously suggested that Chinese companies build vulnerabilities into chips that are exported to the West for use in military systems.
Hardware Trojans

A malicious circuit put inside a chip which is harmless in normal operation until it gets triggered by a preset internal or an external condition.
Anatomy of a Hardware Trojan

Trigger
Events which Enable the Trojan
Stealth depends on triggers

Payload
The Ammo / firepower
Size is not proportional to destruction

Image Source: http://newsblaze.com/cartoon/newsblaze/gv0620c.html
A very Simple Trojan

Towards a comprehensive and systematic classification of hardware Trojans J. Rajendran, et al
Why is Trojan Detection Difficult

• Stealthy nature
  • Low probability Triggers are finite state machines that can change states when **time** or **input data** changes
  • Nano-scale devices and high system complexity make detection through physical inspection almost impossible.
• Test time is expensive.
  • Consider testing a million chips per production batch
  • Even a small chip today has a billion nodes and \(2^{billion}\) States.
  • Test are for known use cases
  • Very difficult to test for **Unknown Unknowns**!
• Large number of gates in modern chips
• Gate Level Simulations are extremely computation and memory intensive.
• Inspection through destructive reverse engineering does not guarantee absence of Trojans in ICs not destructively inspected.
• Audits not very effective at catching bugs

**Key Takeaway #5** : A Hardware Trojan is near impossible to detect in tests because its designed to trigger in mission mode.
Trojan Classification

Source: A Survey of Hardware Trojan Taxonomy and Detection, Tehranipoor et.al
Types of Triggers

Analog
- On chip sensors, antennas used to trigger a malfunction

Digital
- **Combinatorial** triggers generated by logical combination a particular circuit state.
- **Sequential** Triggers are counters/state machine based and re sometimes impossible to detect until the failure mode

Image Source: Hardware Trojan: Threats and Emerging Solutions, Chakraborty et al
Types of Triggers

Analog
- On chip sensors, antennas used to trigger a malfunction

Digital
- **Combinatorial** triggers generated by logical combination a particular circuit state.
- **Sequential** Triggers are counters/state machine based and re sometimes impossible to detect until the failure mode

Image Source: Hardware Trojan: Threats and Emerging Solutions, Chakraborty et al
A simple “Time Bomb”

Trigger: Internal
Payload: Functionality Change
Detection Probability: Low
Codename: Time Bomb

Image Source: Hardware Trojan: Threats and Emerging Solutions, Chakraborty et al
A very Simple information stealing Trojan

Trigger : Internal  
Payload : Information Leak  
Detection Probability : Low  
Codename : Agent X

Experiences in Hardware Trojan Design and Implementation  Yier Jin, Nathan Kupp, and Yiorgos Makris
A very Simple information stealing Trojan
Trojan Detection Approaches

- **Destructive**
  - Scanning optical microscopy (SOM)
  - Scanning electron microscopy (SEM)

- **Non Destructive and Non Invasive**
  - Bulk Current Measurement
  - Bulk Power Measurement
  - Data path delay measurement
  - Reliability Tests like burn in at elevated voltage and temperatures.
  - ATPG scan chains
  - Logic tests
  - Functional Tests (Run time monitoring)
  - Built in self tests

- **Invasive techniques wherein special circuitry is embedded in the chip to aid Trojan detection.**
  - Connectivity signatures
  - Triple modular redundancy
  - Transparent modes for state machines.
  - Improving observability and controllability of internal nodes.
Mitigating the Threat

• Ensuring Authenticity of ICs
  – make the entire Development process trusted
  – Silicon Design Authentication
  – Trust In IC Program (DARPA)

• Design Trustable Hardware
  – Redundancy
  – Obfuscation
  – 3D IC technology
  – Tamper proof designs
  – EDA Tool Support

Key Takeaway #6: Long term research can bring built in security and tamper resistance in IC designs. However, for short term, the threat can be mitigated by making the supply chain trusted.
Questions

Speaker Contact
Asif Iqbal
asif.iqbal@alum.mit.edu
Video Resources

- 40% fake chips in military
  - http://www.youtube.com/watch?v=saghakMnvtw&feature=related

- Chip recycling
  - http://www.youtube.com/watch?v=5vN_7NJ4qYA&feature=related

- Blackhat Videos
  - http://www.youtube.com/watch?NR=1&v=7I7hLHhQ2UQ&feature=endscreen
References

- https://citp.princeton.edu/research/memory/media/
- Cyber security in federal government, Booz Allen Hamilton
- The hunt for the kill switch, IEEE Spectrum, May 2008
- The hunt for the kill switch, IEEE Spectrum, May 2008
- The hunt for the kill switch, IEEE Spectrum, May 2008
- Towards a comprehensive and systematic classification of hardware Trojans, J Rajendran et.al.
- Hardware Trojan: Threats and Emerging Solutions, Rajat Subhra Chakraborty et al.
Levels of Abstractions

HIGHEST LEVEL
- Change protocol
- Constraints
- Additional gates
- Modify layout
- Modify wiring
- System level
- RT level
- Gate level
- Transistor level
- Physical level

LOWEST LEVEL
- Increasing sophistication
- Decreasing Trust
- Increasing ease of detectability

Image Source: Towards a comprehensive and systematic classification of hardware Trojans, J Rajendran et al
DARPA TRUST in IC Program

• “Trusted Foundry Program” provide interim measure for trusted high performance IC’s.
• Certain Circuit topologies and building blocks to be used.
• Design guidelines with respected to debug options, testability, backdoors, TMR etc.
• Techniques that can quickly and accurately determine whether an IC provided is the same as one available in a gold standard design
Agents of Attack

Remote Hackers: no physical access to the device, rely on sophisticated hacking tools.

Security specialist: technically capable attackers are criminal gangs, security experts, and users attacking devices for fun, capable of executing a lab attack.

Trusted developer: Engineers, scientists working for trusted organizations, may be bribed to insert backdoors in design and specifications.

Device Distributor/Fab Owner: In general the device owner is motivated to perform the attack, but is not technically competent. A technical expert will have developed an attack and embed it onsite.