Hardware Trojan Development and Detection using ATPG tools

Abstract
- Hardware Trojans are malicious additions to computer hardware designs that can cause a lack of security
- Increased costs associated with owning an IC fab has resulted in more ICs being manufactured overseas
- As the result of some DoD ICs being produced overseas, a need to test for Hardware Trojans has grown
- Hardware Trojans have a trigger and a payload, triggers are hard to detect, payloads are attacks on circuits
- Using a “Stuck at” fault model with ATPG tools we are attempting to detect hardware Trojans

What is a Hardware Trojan?
Trojan Hardware is in red

What is at risk with current practices?
- Additional Hardware Embedded Maliciously
- Secure Information
  - Provide attacker encryption keys or master keys
  - Leaking secure information or plaintext
- IP – Intellectual Property
  - Circuit Designs
  - 3rd Party IP
  - Licensed Designs

How are Hardware Trojans Inserted?
- Hardware Trojans can be inserted at many points in the supply chain
  - Supply chain is shown in blue
- Possible methods of Trojan insertion is in red

BCD Trojans
- BCDs are used to display decimal numbers with LEDs
- Example of uses: Alarm Clocks, Timers, Power regulator for a F-16 Fighter Jet

MIPS Trojans
- MIPS processor is a general purpose computer processor
- Can be used to run MIPS assembly code
- Trojans – No more instructions
  - Trigger: Add 555, +77777 (using calculator)
  - Payload: Disables instruction input (kills keyboard)
- Trojanz – Memory Cleaver
  - Trigger: Add 888, –9999 (using calculator)
  - Payload: Clears all user data (deletes all files in memory)
- Trojanz – Shadow Registers
  - Opcode = 111111 (part of input instruction)
  - Payload: Copies data in processor then saves in memory

Watchdog Processor Trojan
- Watchdog Processors are used to monitor timed-out processes
- Checks a word registers to ensure equivalence
- If counter times out and the words are not equal, reset occurs
- Trojan:
  - Trigger: Word_input = AFAB
  - Payload: Reset loop does not stop until Global Reset
  - Bottom line: Trojan stops circuit from working
  - Ever had a computer stop working? Annoying, isn’t it?

Conclusions and Future Work
- Research is ongoing
- 6 Trojans have been created for 3 hardware designs
- ATPG tools have been able to detect Trojans
- Currently developing data analysis scripts
- Mentor Graphics tools have been primary focus
- Project will eventually move to Synopsys tools
- How do we identify patterns that detected Trojans?
- Are the patterns functionally valid?