LSIBs and Improving Test Hardware Security

Presented By: Adam Zygmontowicz & Micah Thornton | Faculty Advisor: Jennifer Dworak

Industrial Collaborators: Al Crouch & John Potter of ASSET InterTech | Department: Computer Science & Engineering

On-chip instruments and data shouldn’t be accessible in the field
For example…
- Hidden Chip ID’s help prevent counterfeiting...but if they are read by an attacker, the chip can be cloned and possibly end up in military hardware.
- Region Code keys may be included in chips to allow decrypting of protected video. Making these codes accessible aids in piracy
- Internal instruments, such as trace buffers, allow an attacker to see internal states of the machine and reverse engineer hardware or software

Why is this a problem?
...On chip hardware needed for test and debug (e.g. P1687 access networks) can also be used by attackers!

We need a way to hide instruments/data from unauthorized users.

Our Solution:
- Take advantage of the dynamic data-driven network aspects of P1687 and modify standard SIBs (Scan Insertion Bits) so they become..._Locking SIBs (LSIBs)_

What is a Scan Chain?
- Bits (logic 1 or logic 0) are shifted into scan cells like marbles stuck in a tube.
- Scan cells can send data to the circuit to control it or receive data from it so we can look at it...

What is P1687?
- P1687 uses the data in the chain itself to make the chain longer and access new instruments.
- A new segment is opened if a “1” is present in a special scan cell called a SIB on an UpdateDR.

Add Traps!
- If an incorrect value is in a TRAP bit on an updateDR, it will disable opening the lock permanently until the circuit is globally reset.

If an attacker thinks traps may be present, he needs to pull a global reset after each attempt

The number of shift cycles required per attempt approximately doubles!

Average Cost (unlocking LSIB): T_{trap} = (10 + 2n + d) * 2^n

Hierarchical Configuration
- LSIBs, key, and traps can be behind different LSIBs
- An attacker must unlock multiple LSIBs to get to the hidden instrument
- Traps may be sprung when unlocking one LSIB that keeps you from unlocking another one.

Can we make it even harder?

Increase in Avg. Time Required to Unlock Two Hierarchical LSIBs over a Single LSIB with Traps

What is the area overhead for an LSIB?
- Xilinx Spartan-6 XC50X75T-3FGG676C FPGA
- Used for the implementations of the LSIBs

Conclusions and Future Work
- LSIBs will dramatically improve hardware security by helping protect hidden instruments with low overhead.
- Hierarchical configurations provide further protection against a “lucky first try.”
- Possible Future Work
  - Simple Serial Encryption
  - Extending/Contracting scan chain w/LSIBs and PUTs