Processor Encryption
Towards More Secure and Reliable Processors

Jeyavijayan (JV) Rajendran,
Polytechnic Institute of New York University

“IT Security for the Next Generation”
American Cup, New York
9-11 November, 2011
Hardware Security

Security of Integrated Circuit is critical for most applications

Is the hardware secure? Do you trust it?
Hardware Trojans

Malicious circuitry added without the designer’s knowledge

Sources:
1. Off-shore fabrication houses
2. Malicious in-house designer
3. Hardware Intellectual Property designers
4. CAD tools fabrication houses

Is the threat real?

Short Sharp Science

PC giant warns of hardware trojan

'Hardware Trojans' could turn microchips into timebombs

Google investigating hardware Trojan tech

Creative Winners in Hardware Trojan Contest

Simple attacks and creative defenses
By MARK ANDERSON / JANUARY 2010
Problem of Trojan detection

**Scalability**
- Size of the design – 1000000000 gates
- Trojan size – few gates (< 10)

**Trojan detection**
*(Post-manufacturing)*
- Detect Trojans using
  - Additional power consumption
  - Additional delay
  - Combination of the above
- Works only if the size of the design is <10000 gates

Can any one tell what it actually does?

Tools and methods that ensure the security of the software do **NOT** detect hardware Trojans

How to ensure the security of 1000000000 gates with 10000 secured gates?

Trusted design team:
1. Design a small secure part (<10000 gates)
2. Encrypt * rest of the design
3. Put the keys in the secure part

Attackers if they insert Trojans in
1. Secure part – Easily tested because of small size and so gets detected
2. Encrypted part – Hard to understand the logic and hence can’t insert

* Logic encryption: Insert some additional gates into the design such that only on applying specific inputs to these gates, the design produces correct output
How to ensure the security of 1000000000 gates with 10000 secured gates?

Trusted design team:
1. Design a small secure part (<10000 gates)
2. Encrypt * rest of the design
3. Put the keys in the secure part

Attackers if they insert Trojans in
1. Secure part – Easily tested because of small size and so gets detected
2. Encrypted part – Hard to understand the logic and hence can’t insert

* Logic encryption: Insert some additional gates into the design such that only on applying specific inputs to these gates, the design produces correct output
During working
1. Secure part verifies the instructions
2. Decrypt the encrypted units if instructions are correct
3. Processor executes instructions
4. If instructions are not correct, processor won’t execute them

- An encrypted processor pipeline with Dynamic Trusted Platform Module as a secure part Load Store Unit (LSU) is encrypted.
- LSU is made functional only instructions are correct.
- The OR gate Trojan cannot disturb the secure processor.
Conclusion

- Hardware Trojans are emerging threat
- Current approaches cannot detect them
- Designed a scalable approach to thwart Trojan attacks in processors
- Security through obscurity
- Solution is applicable to large design houses, fabless companies, etc..
- Our results showed that the performance overhead is around <0.2%
Thank You

Jeyavijayan Rajendran,
Polytechnic Institute of New York University

“IT Security for the Next Generation”
American Cup, New York
9-11 November, 2011

... and that concludes my talk, now I have to put you all under arrest for possessing classified information!
... and that concludes my talk, now I have to put you all under arrest for possessing classified information!