How to Protect Your Device from Hardware Trojans

Sudeendra kumar K and K K Mahapatra
National Institute of Technology, Rourkela.

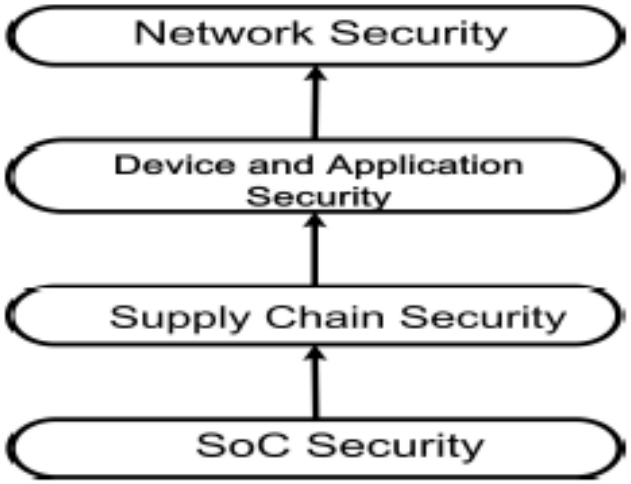
Real-World IoT Security Conference
2017
Bangalore

IoT Design Tenets

- The idea of Internet of Things (IoT) is to connect the digital and physical worlds seamlessly to create a network of objects which communicate with each other. There can be millions of objects in the network with a capability to take intelligent decisions.
- The core tenets to follow in the IoT design are: - agility, scalability, cost and security. Security is of a prime importance because it is a part of challenge and also it is one of the core tenets in the IoT design.
- The known challenges in an IoT ecosystem are: -
  - Identification or authentication for addressing an IoT node.
  - Choosing a right connectivity technique.
  - Maintaining data compliance across network and security.

Security and Electronics Gadget

- Security design should be comprehensive and cover all layers from things to cloud. The comprehensive security solution should address: - data integrity, data provenance, identity or authentication of things, trust management and user privacy at all levels from things to cloud.
- In IoT security, to address the security issues at every layer, root of trust should come from hardware. SoC/microcontroller targeted to IoT applications support encryption of data transactions, authentication of device/things through crypto IP.



Hardware Security

- The well known hardware security threat from last two decades are different types of side-channel attacks and reverse engineering. Side-channel attacks are primarily performed on cryptographic implementations to extract the key used in encryption. Power based side channel Analysis is most widely discussed in security community and recent additions are timing attacks, fault attacks and electromagnetic attacks.
- Globalization of semiconductor industry has brought changes in design, manufacturing, test and EDA. The supply chain/service chain is fragmented across geographies and this resulted several hardware security related issues like: -
  - Counterfeiting
  - Hardware Trojans
  - IP violations

Hardware/Firmware Trojan

- Hardware Trojans are defined as malicious modification of a design which leads to unexpected behaviour. Intentions of an adversary who perform malicious modifications can be leaking sensitive information, denial of service and degradation of performance.
- In 2008, Adee [2008] reported that a critical failure in Syrian radar might have been intentionally triggered through a “back door” hidden within a commercial off-the-shelf (COTS) microprocessor.
- According to a U.S. defense contractor who spoke on condition of anonymity, a “European chip maker” recently built such microprocessors with remote kill switches for just such purposes.
- Given the dire consequences associated with such weaknesses, the so-called hardware Trojan issue has received considerable attention from academia, industry, and government over the last decade.

Reference: S. Adee. 2008. The hunt for the kill switch. *IEEE Spectrum 45, 5 (May 2008), 34–39. DOI:http://dx.doi.org/* 10.1109/MSPEC.2008.4505310

Hardware Trojan Insertion

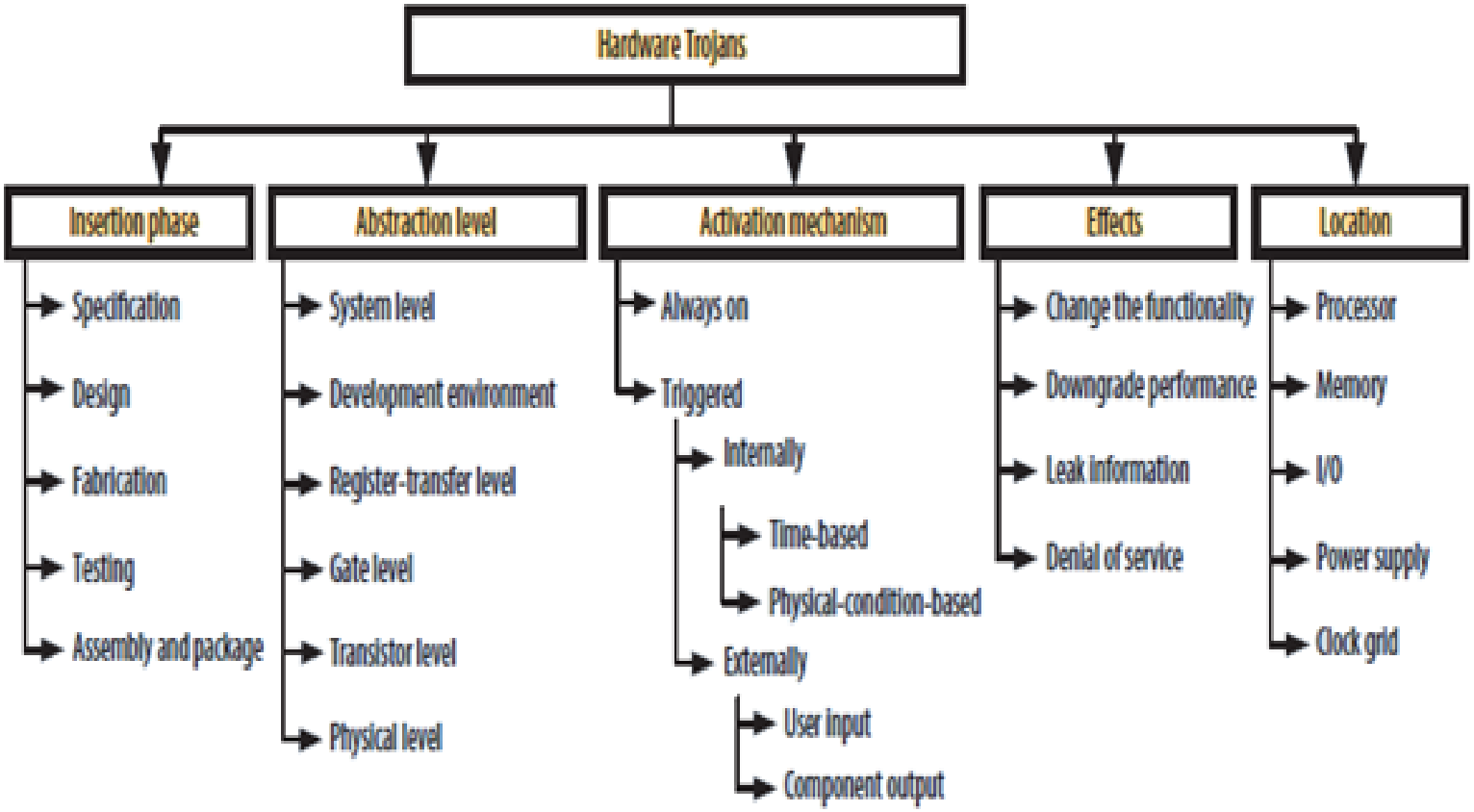
Description	RTL (Soft IP)	Layout Design (Hard IP)	Research literature
3PIP	Yes	Yes	80% of literature available studies the HT insertion during RTL design
In-house (SoC design house) IP development team	Yes	Yes	
SoC Bus design/Integration team	Yes	Yes	2 papers deal with HT's in SoC bus architecture.
Test design/DFT of a SoC	Yes	NA	No literature found.
Layout/Physical design of SoC including global resources: clock and power supply.	NA (Not Applicable)	Yes	HT insertion during physical design which target reduction in reliability and Denial of Service .

Hardware/firmware Trojan Design

An adversary will design the malicious code in such a way that: -

- Hardware Trojan will go undetected during rigorous verification processes like functional coverage, code coverage, assertion driven verification etc.
- Generally, it is assumed that, Hardware Trojan is triggered for a very rare event, which may be missed as corner case during verification.
- Hardware Trojans will never affect the functionality or any kind of specification of design.
- The common and well known intentions of adversary are: - leaking secret information by promoting side-channel attacks, denial of service etc.
- The intentions of adversary vary from design to design based on this functionality.

Hardware Trojan Design and Taxonomy



Pre-Design and Post-Design Hardwar Trojan Detection

Description	Pre-Design HT detection	Post-Design HT detection
Technique	Several techniques based on functional verification, formal verification and Boolean SAT methods.	Functional test, destructive reverse engineering and side-channel analysis methods.
Probability of Detection	It is difficult for an adversary to hide the HT which will escape functional and formal verification, Synthesis, Power and Timing analysis in a complete ASIC design flow. Probability of HT detection is less than 50% without specialized HT detection scheme.	Theoretically, it is possible to detect all types of Trojans, given an enormous amount of time, sophisticated equipment and expertise. Testing for HT during production testing on ATE is nearly impossible with current technology.
Cost	Less cost involved	Expensive.

Survey of HT Detection Techniques at RTL level

Description of HT detection technique	Remarks
Unused Circuit Identification (UCI) creates a data-flow graph of a design and generates a list of all data-flow pairs, through which data flows from a source signal to a sink signal.	The UCI is similar to Code coverage in industry standard tools.
FANCI defines a metric called control value to identify the nearly unused logic. The control value is used to find the malicious logic or backdoors.	FANCI fails to detect HT's with multi-cycle trigger/activation.
FASTrust: - HT feature database is created using the available taxonomy of Trojans. The feature analysis of a design or 3rd party IP core is performed after extracting the flip-flop level Control Data Flow Graphs (CDFG) of design/IP core. The feature matching algorithm is used to detect the nodes or node groups similar to HT features in the design with the help of database.	The handicap of FASTrust is designing optimal database.

Defense Strategies

HT attacks on microarchitecture like:-

- Sudden change in the value of Program Counter (PC).
- Changes in clock features, glitches etc
- Accessing a confidential memory sections.
- Application program executing privilege commands like factory settings etc.
- Fluctuations in power supply to the internal circuit /modules of the microcontroller.
- Run monitoring of all vital assets and abnormal system behavior is key in HT defense.

How to choose a microcontroller for IoT (Security)

- At present, security concerned with IoT is dealt at software level or application level. For the success of IoT the root of trust and security build-up must from the hardware.
- Microcontroller used in IoT, ideally should support: -
  - Encryption of vital data transactions between processor, memory and external world.
  - Authentication and Identification of device, which is useful in IoT authentication and as an anti-counterfeiting technique.
  - Run-time monitoring unit to monitor the vital asset with minimal effects on performance of the microcontroller. (Defence against Hardware Trojans).
  - The Debug instruments are used to extract the secret keys. The microcontroller should have appropriate debug security mechanism to protect vital assets of system.

Summary

- In chip design, along with basic tenets : Area, Power and Timing, the security is a new addition, which industry can’t ignore.
- Very importantly, microcontroller/SoC targeted for IoT applications must have a dedicated on-chip infrastructure for security to address the security of IoT comprehensively.
- In the FPGA based IoT applications, the IoT makers must take care of all varieties of security threats known.
- The chip makers not only for IoT applications, all their products should carry a dedicated security block, which is beneficial to both the end user and chip maker.

Future on IoT Security (Hardware Trojan)

- There is lot of active research in both industry and academia to address the security issues of IoT.
- Physical Unclonable Functions (PUF) may play a vital role in anti-counterfeiting, protecting IP rights and authentication of IoT's.
- Run time monitoring is crucial not only against Hardware Trojans, but in general it is important in IoT security.
- Still understanding of Hardware Trojan is not on the solid foot. There is a lack of generic definitions of hardware Trojan structure, etc. Research in Benchmark Hardware Trojan design and analysis is crucial in the Trojan study.
- Hardware Trojan detection and Defense mechanisms need a constant progress with the advent of new varieties of hardware Trojans and hardware intrinsic security threats.

Thank You