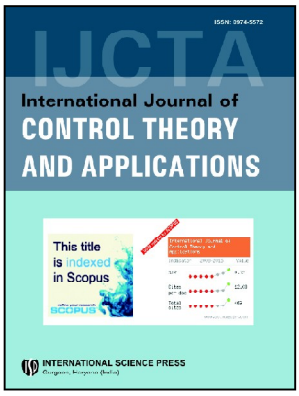

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 21 • 2017

Emerging Hardware Trojan Threat to Integrated Circuits -Remedies to Protect the Integrated Circuit

***Vuyyuru Tejaswi, A. Surendar, N. Srikanta and Gudapati Ramyasri**

* *Department of Electronics and communication engineering, VFSTR University, India, E-mail: tejaswireddy.456@gmail.com*

Abstract: Due to growing of semiconductor industry and the increasing demand in fabricating digital integrated circuit, are now facing problem with a hardware threat which is known as hardware Trojan horse. Hardware Trojan (HT) results in harmful, unauthenticated modification to integrated circuit (IC), which is a major part of electronics. The modification may leak important information ,causing the system to fail while operating in real time. HT has been found as a problem to military, medical, transportation and other critical systems. It is a major security threat for the integrated circuits like FPGA, ASIC, Microcontroller, microprocessor .Hence it is a major security challenge to prevent and detect the hardware Trojan. In this regard first one have to know the ways in which this HT can be encountered. The most significant way to handle this Trojan problem is to understand the Trojan classification and counter attack techniques. A new taxonomy was presented in this paper to handle the HT, this classification covers the prevention and detection methods.

Keywords: Hardware Trojan horse, Integrated circuit, HT prevention and Detection

1. INTRODUCTION

Electronics plays an important role nowadays. In our daily life we depend on electronic gadgets like USB, Smartphone's, computers, etc for storage and communication of confidential information. In all these electronic devices there will be an integrated circuit .Since IC'S are major building block of electronic devices. They are used to implement a specific function. The ability to trust these IC's have become a security concern because without having belief on this IC's,the devices which contain them cannot be believed. A security threat which is known as Hardware Trojan is attacking the electronic devices particularly IC. A Hardware Trojan horse is intentional change made to the integrated circuit design which results in incorrect operation of device [1]. The main differences between hardware Trojan and software Trojan is in hardware Trojan once the Trojan is inserted in to the IC the Trojan behavior cannot be changed. Whereas in software Trojan ,the Trojan is part of the code in software and the Trojan behavior can change. A software Trojan is added to a software through network. Hardware Trojan threats must be identified earlier in integrated circuit design flow. Proper prevention and detection methods must be followed to get rid of this hardware Trojan to some extent.

This paper is divided into sections like, in Section 2 we describe the IC design flow and chances of Trojan insertion in the IC design flow. Section 3 elaborates about hardware Trojan horse and their taxonomy. Section 4

and 5 describe about the new classification i.e; prevention and detection of hardware Trojan and finally section 6 offers the conclusion.

2. IC DESIGN FLOW

The design of an IC comprises several steps. The first step is the conversion of specifications/requirements text in to architecture design and then writing in any of the Hardware description languages like verilog/VHDL and the test bench is written to make sure that the HDL description for the device is correct or not. Then the synthesis stage is used to generate a netlist. The place and route or layout in implementation stage is used to give the netlist a physically realized form. The digital file which is produced is handed to fabrication. After producing the actual circuit by industry, the testing step checks for correct operation of the circuit and after the assembly and packaging step, the circuits are headed for use. Fig. 1 shows there is a chance of hardware Trojan horse insertion at design, synthesis and fabrication stage.

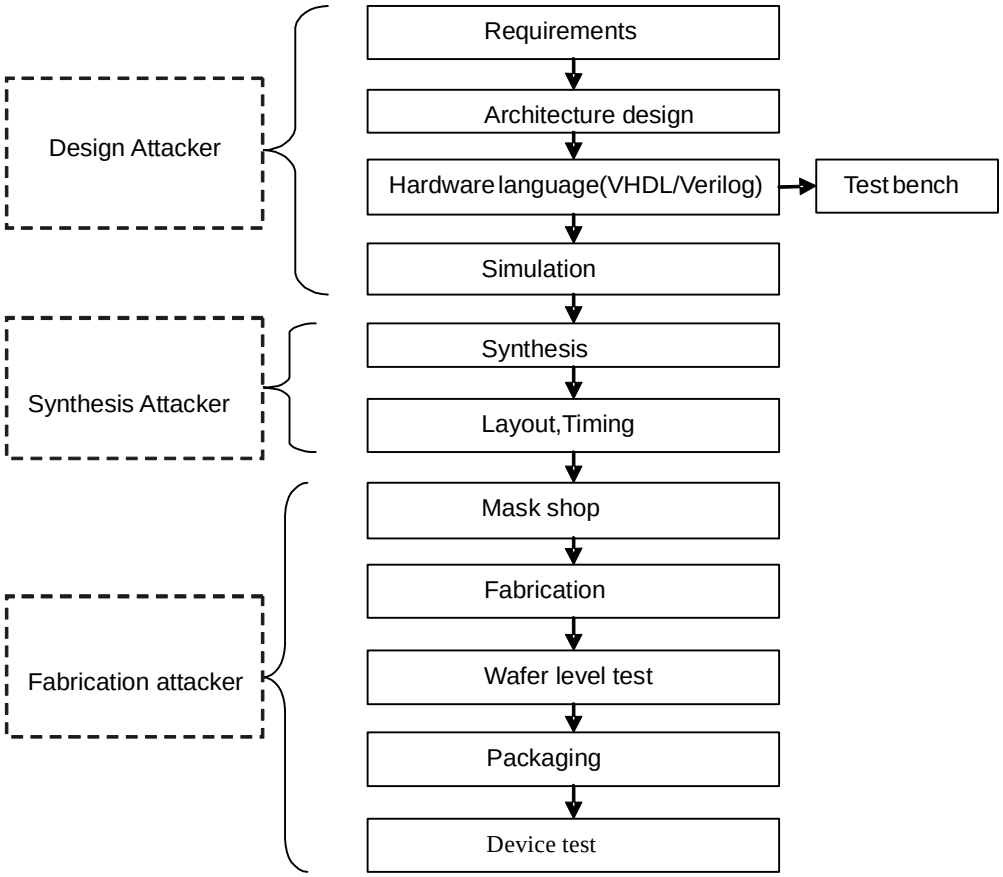

Figure 1: IC development cycle

3. HARDWARE TROJAN TAXONOMY

Hardware Trojan Horse (HTH) consists of two elements which are Trigger and Payload. Trigger, activates or enable the malicious activity. Payload is used to run the malicious activity. HT serves as Time bomb Trojan which disables the device at some future time. It can also serve as a data exfiltration Trojan which leaks confidential information over secret channel. In the Hardware Trojan classification, the adversary has access to all stages of the IC.

A. Through what ways hardware Trojan is incorporated in the design phase?

1. First comes the Specification phase, in this features like expected function, power, delay and size are defined. Here the Trojan might change hardware timing requirements.
2. In the Design phase, the designer uses the standard cells and third party blocks. Since we are relying on third party and standard cells there is a chance of hardware Trojan insertion in that.
3. In the Fabrication phase severe effects occurs when there is Subtle mask changes .However during extreme cases the attacker could replace it with different mask set.
4. Next comes the Testing phase, in this test cases are generated through Automatic Test Equipment(ATE) to the IC. The adversary changes the test vectors to make Trojan detection difficult.
5. In the Assembly and Package phase the IC which is tested and other components are assembled on printed circuit board. The adversary have a chance of inserting Trojans into the interfaces during packaging.

B. Through what ways hardware Trojan is inserted in the abstraction phase?

1. At System level Trojans can be triggered by hardware module. Example: By exchanging the ASCII values of keyboard inputs

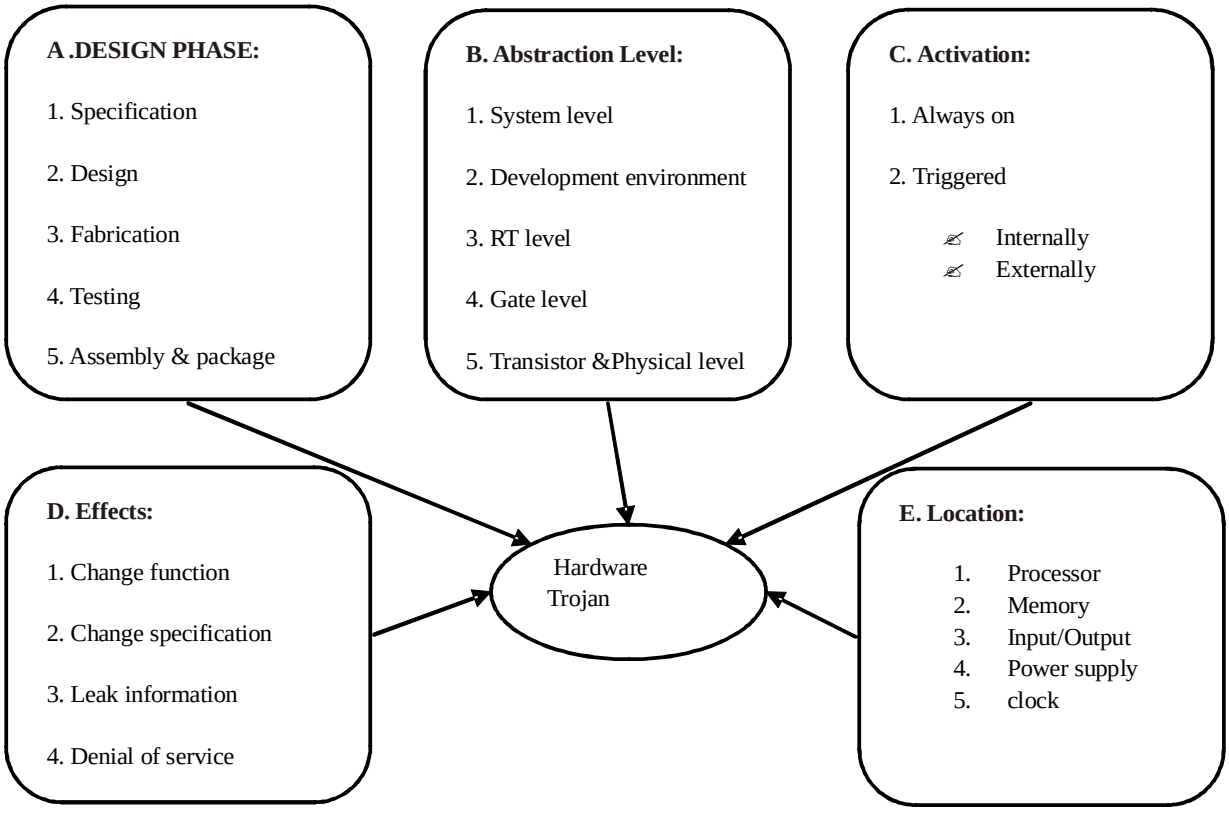

Figure 2: Hardware Trojan Taxonomy

2. At Development environment an adversary can use CAD tools to insert Trojans.
3. At RT level developers describe each functional module in terms of registers, signals and Boolean functions.

4. At gate level the design is represented in the form of interconnection of logic gates. Here trojan can be a comparator having xor gates which is used to monitor the internal signals of a chip.
5. The transistors are mainly used for building logic gates in transistor level. Transistors are added or removed to modify circuit functionality. To change circuit parameters transistor sizes are changed.
6. Last comes the physical level in this Trojan can be inserted by adversary by modifying the layout and wiring.

C. How a Trojan will be activated?

Some Trojans will be always on while others will be triggered when an event like internal or external arises. On the occurrence of event only Trojan will be activated. Once triggered they remain active forever or remain dormant for some time.

1. The Internally triggered Trojan gets activated by an event which occurs within the target device. In this the event can be of time based or physical condition based. Time bomb comes under time based. The physical condition based Trojan will be activated when it exceeds the physical conditions such as temperature, humidity, atmospheric pressure. For example when a chip temperature exceeds 56 degree centigrade a Trojan will be triggered.
2. An externally triggered Trojan will be activated when the target module receives external input. The input can be of user input or it can be component output. The User input can be switches, pushbuttons and keyboards.

D. Effects of a Hardware Trojan?

Trojans results in undesirable modifications to the system. Their effects range from small disturbance to the critical system failures.

1. Changing the function of the hardware device by a Trojan results in some precise errors which is hard to detect.
2. By modifying the specifications like delay, size and power the trojan can change.
3. Trojan also leaks important matter. Information can be leaked through interfaces like RS232, JTAG and also by optical and thermal.
4. Denial of service Trojan results in preventing the operation of a function. For example it causes the processor to bypasses the interrupts occuring from peripherals.

E. Location of trojans?

Trojan can be incorporated in one or many components. Trojans can be located in a processor, memory, Input/ Output units, power supply and clock. Trojans inserted in multiple components can act independently or even as a group.

1. A Trojan incorporated in the processor may change the order of execution of instructions.
2. A Trojan in the memory alter the values stored in memory. One example is a Trojan might change the PROM values in an integrated circuit.
3. A Trojan can be there in the printed circuit board and even in the chip peripherals. If a Trojan is inserted in the RS-232 module then for data transmission the baud rate is higher than the original 9600 baud rate which results in leakage of sensitive information.

4. In power supply units Trojans change the voltage and current supplied to the device and results in failure of a device.

5. Trojans inserted in the clock grids changes the clock frequency

Validation for the above mentioned taxonomy can be referenced in [2].

4. PREVENTION

One way to protect the design against trojan is by preventing them from being incorporated in any stage of integrated circuit design flow. It is always best to use trusted synthesis and simulation tools for designing and also fabricating in trusted foundry so that there will be less chances in malicious modifications. The prevention can be done in design, layout level, Fabrication stages of an IC development cycle [1].

(a) Prevention at Design stage: Prevention at this stage can be done by avoiding use of untrusted EDA tools and untrusted third party Intellectual Property(IP) blocks in the design . One way to avoid Trojans at this stage is to use all the hardware resource at all the times that is on all clock cycles. All the resources must be used properly in such a way they are required to satisfy the correct function of an integrated circuit.

(b) Prevention at Layout level: Circuit layout containing unused spaces, unused routing channels and noncritical paths are more susceptible to hardware Trojan insertion.

Prevention against hardware Trojan can be done by filling the unused spaces in the layout of a design with functional standard cells instead of non-functional filler cells this is done by using a technique called BISA [7]. The unused space can also be filled by flip-flops, multiplexers, lookup tables by using a technique called dummy logic [3]. While filling this unused space some routing issues arises so some routing algorithm must be developed to tackle down this problem.

(c) Prevention at Fabrication: Prevention at this stage can be done by avoiding fabrication from untrusted foundries. Jin and Makris proposed a system that has IP consumer providing security related properties. IP consumer and IP producer must agree to those properties translation to get rid of the Trojan.

5. DETECTION

It is not completely possible to prevent hardware Trojan horse insertion in an IC design. Nowadays currently lot of research is going on the detection of hardware Trojan which is gaining lot of significance.

Hardware Trojan detection approaches are of two types destructive and non-destructive. In destructive method of hardware Trojan detection it fully destroy the integrated circuit.The integrated circuit must be completely reverse engineered to ensure that there is no trojan in IC. However reverse engineering a complex integrated circuit is time consuming process. However reverse engineering of an IC means analyzing the integrated circuit internal structures and their connections , to know how it is designed and is operated. A reverse engineering flow includes the following they are de-capsulation, de-layering, image reconstruction, annotation, schematic creation and analysis.

Destructive method is costly and very time consuming The Trojan can enter in to the circuit by adding or by removing the logic gates. Due to high costs of destructive detection mechanism we came for nondestructive mechanism. The nondestructive mechanism will not destroy the IC being examined. Non destructive mechanisms are of invasive and non-invasive. In Non-invasive mechanism the design is unchanged, whereas invasive mechanism modify the design. Non-invasive technique is again of two types run time and test time ,under test time there are logic test and side channel

Run Time Monitoring Approach

Detection of all types of Trojans during post silicon test may be infeasible practically ,so online monitoring of critical tasks can increase the trust level with respect to Trojan threats. On detection of any malicious logic or function change these run time approach disables the chip or bypass it and allows only reliable operation. One such online monitoring approach is addition of reconfigurable logic, which is referred to as DEsign For Enabling Security(DEFENSE)logic in the soc to enable real time monitoring. When any malicious deviation from original circuit function is observed this approach identifies it and the reconfigurable logic implements the infected logic function and it in turns disable or bypass it. A combined hardware-software approach has been proposed for hardware Trojan detection. This approach attempts to detect DOS (Denial Of Service) attack, this can be detected by using hardware guards which sits on memory bus.

Logic Testing method

Constructing a test vector to cover the entire logical space in an integrated circuit is computationally infeasible. So to overcome this some statistical approach is followed [5]. Logic testing performs checking at the pre-silicon design stage and it includes generation of test patterns through Automatic Test Pattern Generation(ATPG) in order to excite critical paths during testing of a chip. Based on IC's logic structure analysis this method is divided in to functional behavior analysis method and find hidden features method [6].

Coming to the functional behavioral analysis test vectors are inserted in to the inputs of electronic circuit and the output is observed. If the output is not compatible with the input then a deviation/modification is recognized. This method is generally used for detection of functional errors and detection of parametric hardware Trojan(hardware Trojans are added by modifying the structure of the circuit) and cannot detect functional hardware Trojan(hardware Trojans are added by adding/subtracting some elements in the circuit).The disadvantage of this logic test functional behavior analysis method is large scale of test environment in integrated circuits. To overcome this disadvantage Jha proposed a method which is based on Randomization.

Side Channel Analysis

This method detects hardware Trojan by observing the change in circuit Parameters because hardware Trojans generally results in modification of circuit parameters like power, timing, delay, temperature, sound, electromagnetic wave and current . By comparing the above mentioned circuit parameters with healthy and suspicious chip we can detect hardware Trojan. In power based analysis the Trojan is detected by comparing the golden integrated circuit (which is Trojan free) with integrated circuits that are required to be authenticated .If they match then that integrated circuit is Trojan free and is authenticated. If they did not match then that integrated circuit is considered as suspicious. The power signature of golden IC can be obtained by applying many input vectors to the circuit to yield a power spectrum which is basically taken as reference. The circuit is divided into areas and random vectors are applied and power spectrum is estimated for each area [4].

The current that a Trojan can get is very small and it can be hided into the noise and process variation effects and it is not detectable by conventional measurement equipment. However detection of Trojans can be done by measuring the currents locally and from many power ports/pads. The more information can be obtained from [8], [9]. The Trojan included in a circuit results in variation of size of transistor and number of logic gates. Hence the size of the capacitor changes in specific routes, the route delay, fall and rise times will also undergo change. The delay or frequency is measured to distinguish healthy one from the suspicious circuit which is mentioned in [10], [11], [12]. Merging of power, delay and current has been applied in [14],[15].Although side channel analysis method is low cost ,there are disadvantages like the nanometer chip dimensions led to smaller circuit currents which are wrongly considered as noise. This is applicable to delay also.

For the Trojan not to be detected or identified by any power and delay based techniques Trojan triggers and payloads must have two characteristics: They are:

1. Should be connected to nets with low transition probability
2. Trojan should be placed on a path in such a way that the path with maximum delay is not a critical path.

Table 1
Advantages & Disadvantages of all detection techniques

Sl. No.	*Detection Methods*	*Advantages*	*Disadvantages*
1.	Logic Testing	• For detecting small Trojans this method is effective. • Robust under process noise	• Large Trojan detection is challenging • Test vectors generation is complex
	Functional behavior analysis	Used for detection of functional errors and Parametric hardware Trojans	• Cannot detect functional hardware Trojans. • Entire test is impossible in large ICs
2.	Side Channel	• For detecting large Trojans this method is effective • Testvectors generation is easy • Cost is low • High Performance	• Small Trojan detection is challenging • Not robust under process noise • Requirement to Golden IC
	Delay Analysis Power Analysis	• Reliable and so used in security systems to protect the system against the Trojan.	Measurement of short path is difficult Undesired effect of noise and process variations in measurement
3.	Multiple parameter side channel analysis	• Complex Trojans are detected effectively under the process induced parameter variations • This method along with logic testing provides reliable and effective detection of trojans of almost all sizes and types.	For small Trojans this method will suffer due to reduced sensitivity
4.	Reverse Engineering	For Trojan detection this method is reliable	• High cost • For complex IC it is Time consuming • Not suitable for large scale Trojan detection
5.	Built in self-test(BIST)	• Tests hardware with our requiring any external test equipment • Produce accurate results • Runs at the expected speed of clock • providing better security	This provides fault detection but does not provide fault Isolation
6.	Temperature variations based hardware Trojan detection through ring oscillator	• This method is effective for small scale Trojans with small number of trigger points. • Used as complementary to side channel analysis based detection	High false alarm probability

6. CONCLUSION

This paper provides information about Hardware Trojan, which is currently continuing threat to electronic devices present in the world. The ideal way to tackle down this problem is to clearly understand about the classification of hardware Trojan and their counter attack techniques. A new classification was proposed that is prevention and detection. The prevention and detection techniques are mentioned with their advantages and disadvantages. Having clear idea about the prevention and detection techniques and using the appropriate method at the right place one can protect the electronic device from hardware Trojan. The future work is to develop efficient delay and power based detection techniques to detect the hardware Trojan.

REFERENCES

[1] MarkBeaumont, Bradley Hopkins and Tristan Newby "Hardware Trojans-Prevention, Detection,Countermeasures"

[2] J. Rajendran, E. Gavas, J. Jimenez, V. Pitman and R. Karri "Towards a comprehensive and systematic classification of hardware Trojans".

[3] Behnam Khaleghi, Ali Ahari, HosseinAsadi, and SiavashBayat-Sarmadi "FPGA-Based Protection Scheme against Hardware Trojan Horse Insertion Using Dummy Logic IEEE embedded systems letters, June 2015.

[4] RadR, PlusquellicJ, TehranipoorM. Sensitivity analysis to hardware Trojans using power supply transient signals. IEEE International Workshop on Hardware-Oriented Security and Trust. 2008 Jun; p. 3-7.

[5] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, and S. Bhunia, "MERO: A statistical approach for hardware Trojan detection," in Cryptographic Hardware and Embedded Systems-CHES 2009, ed: Springer, 2009, pp. 396-410.

[6] Ehsan Sharifi, Kamal Mohammadiasl, Mehrdad Havasi and Amir Yazdani "Performance analysis of Hardware Trojan detection methods". International Journal of Open Information Technologies ISSN: 2015.

[7] Xiao K, Forte D, Tehranipoor M. A Novel Built-In Self- Authentication Technique to Prevent Inserting Hardware Trojans.Computer-Aided Design of Integrated Circuits and Systems, IEEETransactionson.2014May; 33(12): 1778-91.

[8] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," IEEE Des. Test Comput., vol. 27, no. 1, pp. 10–25, Jan./Feb.2010.

[9] X. Wang, H. Salmani, M. Tehranipoor, and J. Plusquellic, "Hardware Trojan detection and isolation using current integration and localized current analysis," in Proc. IEEE Int. Symp. Defect Fault Toler. VLSI Syst., Boston, MA, USA, 2008, pp. 87–95.

[10] S. Jha, "Randomization based probabilistic approach to detect Trojan circuits," in High Assurance Systems Engineering Symposium, 2008. HASE 2008. 11th IEEE, 2008, pp. 117-124.

[11] Agrawal D, Bostor N, Yaghma N. Trojan detection using IC fingerprinting. SP'07, IEEE Symposium on Security and Privacy, 2007, IEEE. 2007 May; p. 296-310.

[12] Jin Y, Makris Y. Hardware Trojan detection using path delay fingerprint. 2008 HOST, IEEE International Workshop on Hardware-Oriented Security and Trust. 2008 Jun; p. 51-57.

[13] Hu K, Her N, Kim C, Cheng K. High-sensitivity hardware trojan detection using multimodal characterization. IEEE, In Design, Automation & Test in Europe Conference & Exhibition (DATE). 2013 Mar; p. 1271-76.