Hardware Trojans: An Austere Menace Ahead

Anupam Tiwari and Chetan Soni

Abstract Hardware Trojans, a relatively unheard threat viz-a-viz the typical software-based malwares and virus attacks that keep betiding across is being realized gradually by the IT security domain including the users, the IT Security professionals, and the corporate sector who all of a sudden discern the immense threat they might already be living in with. A distinctive dormant Hardware Trojan threat can be so flagitious that the victim does not even know if he is effectuated when he might already be. Hardware Trojans are evolving threats that can shake the roots of any set and constituted government or corporate giant for that matter. Unlike Software virus/malware threats, Hardware Trojans are pertinacious in nature. This paper brings out an overview of these threats including classifications, mechanisms they work on and the current set of countermeasures being researched upon.

Keywords Integrated circuits · Hardware · Trojans · Threats · Networking threats IC fabrication · Backdoors · System on chip · Trojan side channel

1 Introduction

We all are purview to the City of Troy story wherein few hundred years back, Greek soldiers undertook many attempts but unsuccessfully to capture the city of Troy. Eventually, they departed, leaving behind a large wooden horse, ostensibly as a gift. The citizens of Troy were too happy to accept the wooden horse but as it had to come about; a group of Greek soldiers came out of the horse late night handily and opened the gates for their paisanos, who easily dismissed the quiescent city.

A. Tiwari (✉) · C. Soni
National Informatics Centre, Ministry of Defense, New Delhi, India
e-mail: anupam.tiwari@nic.in

C. Soni
e-mail: chetan.soni@nic.in

M. U. Bokhari et al. (eds.), *Cyber Security*, Advances in Intelligent Systems and Computing 729, https://doi.org/10.1007/978-981-10-8536-9_34

Come to present, Trojan [1] as a term today is synonymous more with the IT Security incidents that have seen a phenomenal increase over a decade. For over a decade now, the IT Security domain loyalists have dedicated their energies, resources, domain knowledge, brainstorming sessions and investments into ensuring that the security is ensured for the user. And so the market today got an overplus of options too, viz., antivirus solutions, Firewalls, Internet Security Editions, UTMs, and the list goes on. These may be different technically in operating but there is one common thing in all these options that they all have a mechanism to detect the threats which are all software based. They have no way, no mechanism to thwart, or even think to detect a threat which is embedded deep inside the IC hardware. A threat is so obliterated to be seen, so unthinkable that for the panic struck solution providers it is like where to start from? How to do? What to do?

2 Defining Hardware Trojan

A Hardware Trojan [2] is a designed alteration of an IC ensuing in the undesired conduct of an electronic device when desired to be in operation with a malicious intent without the knowledge of the user. This undesired conduct in the IC may take any of the forms, viz., Logic Modification which might involve placing an additional logic gate with an optional activation programmed to give unlooked-for output signal leading to overall error result or it can be an Electrical modification that would falsify the timing characteristics of IC by doing Extra capacitive loading on a circuit path.

2.1 Hardware Trojans: Origin and Penetration

Hardware Trojan came into being primarily imputed to outsourcing the fabrication and design to third parties attributed to the huge scales of requirements and economies involved. Now, this small modification can be in place anywhere of a corporate house infrastructure, household chores appliances, or even military and defense COTS equipment.

2.2 Hardware Trojan Security Significations

The austere consequences of Hardware Trojans are well left to the imagination of what holds on to be excluded today in the increasing scenario where dependence on IC and SoC is only increasing. The key heads affected and vulnerable to such attacks may include Logistics Systems and Support domain, viz., Transport infrastructure, Traffic Control, Metro/Rail monitoring and control, Civil critical

applications, viz., Banking, Stock market IT infrastructure, Military Systems viz Weapon control systems, Satellite controls, Radar systems, Surveillance Systems, Decision support systems, Aviation and Aeronautics industry or Miscellaneous domains like Data centers IT infrastructure, Personal info stored in Clouds, Government systems in critical setups, etc.

2.3 Hardware Versus Software Trojans

As brought out from the above about HT, the comparison between severity viz-a-viz Software Trojans allows HT to take leaps out-front lead. It empathizes that the software threats that exist with us over decades now are yet to get a stable and an assured solution by any means and this HT threat has just arrived in the fora. A mini comparison [3] between the two is bought out in the figure below:

Attribute	Hardware Trojans	Software Trojans
Agency involved infecting	Prefabrication embedding in the hardware IC during manufacturing or retrofitted later	Resides in code of the OS or in the running applications and gets activated whilst execution
Mode	Third-party untrusted agencies involved to manufacture ICs in various stages of fabrication	Downloading malicious files from the Internet or via social engineering methods executing malicious files or commonly sources USB, etc.
Current Remedial measure available	Currently none, since once embedded there is no way to remove the same other than destroying	Signatures released by antivirus companies and software patches based on behavioral pattern observed

3 Hardware Trojan Systematics

A hardware Trojan to operate needs ground and power supply which can be low or high depending on the design it is based on. A Trojan that requires a low-end power supply will have low chances of being detected whereas a Trojan requiring higher power supply would invariably be at a larger chance of detection by a sensor if placed. Hardware Trojans have a range of classification based on various characteristics and modes they work in. The classification keeps on evolving as more newfangled approaches and dimensions of attacks are detected. A form of classification based on the activation mechanism of triggering the attack that can be Digital or Analog. Analog will typically get activated based on any analog input type like Temperature, Pressure, time-lag etc. whereas digital will be based on some kind of Boolean logic function [4] has classified the same in another manner as shown in Fig. 1. The classifications as shown are to some degree perceivable by

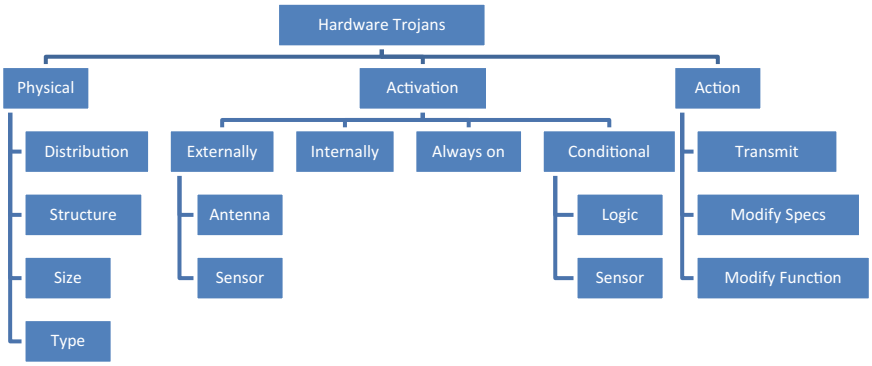

Fig. 1 Taxonomy of Hardware Trojans [1]

their names and depict a very basic and broad classification of the HTs. Another classification [5] divides Hardware Trojans into two types that include Parasite-Based HTs and Bug-based HTs. A parasite based HT hides in the original circuit without altering it and is not involved to lose any set and defined functionalities in the circuit whereas a Bug-based HT not only alters the circuit but also causes it to lose its set and configured functionalities. Of the two parasites HTs become more difficult to be detected through owing to hidden nature and is actually untraceable in specified specs as well as testing.

4 Nemesis Framework

Hardware Trojans insertion would actually gain a large mileage and suit to bestow maximum scathe in a typical supply chain which essentially consists of unalike and miscellanea of insertion points. Hardware Trojan-infected hardware would be more apt for a larger organization and a huge victim base since it will allow a deeper penetration in terms of the scale of victims.

4.1 Hardware Trojan Structure and Mechanics

A typical HT will have primarily two components including a Trigger and a Payload [6]. The trigger part is used to set off the malicious action while the payload is the malicious part that really accomplishes the vicious action. Before a triggering action takes place in an IC, the Hardware Trojan lies peacefully abeyant without any activity and pings anywhere.

Vide [6], the triggering action for a Network Hardware Trojan is shown associated with the LED light of Ethernet controller acts as a method to interpret the

packet timings. The activity LED light seen in general flicking gives a broad indication of the current network traffic presently user is involved with. The [6] has taken the RTL88111E chip for the study which deciphered that there is 160 ms delay between the LED Light to cycle on and off and it is this 160 millisecond delay during which there is no network activity. This timing behavior of this LED activity is used as a trigger for the Hardware Trojan.

Further to this [7], demoed the payload execution with the ENW02A-1-BC01 Gigabit Ethernet PCI-Express card. The network hardware Trojan was shown degrading the network services using noise injection in chips clock circuitry of the Ethernet controller in the form of a bias voltage. The demonstration included desynchronizing the clock of the Ethernet controller chip owing to changes in the affected bias voltage that lead to the changes in the resonant frequency on the external crystal. Vide [8], HT can be an elementary alteration to the original IC. This refers to an insertion of two input AND gates wherein while the HT is inactive the IC gives the desired output unaffected while the same gives an always zero output irrespective of the input given. They referred this particular example as *Stuck at Zero* Trojan, i.e., SAZ.

5 HT Insertions

Hardware Trojans can actually get inserted at various stages of their life cycle typically during design and manufacturing process or maybe even retrofitted to an existing Hardware IC.

5.1 Design and Manufacturing Process

Economic inducements have goaded the semiconductor industry to dissever the design of IC from fabrication. This has allowed potential vulnerabilities from suspicious circuit foundries to covertly embed malicious HT into the erstwhile original design. In the typical design process involved in Application-specific integrated circuit (ASIC), the semiconductor intellectual property core (IP core), i.e., the reusable unit of chip layout design which is an intellectual property of one party or may be licensed to another and Standard model cells wherein low-level very-large-scale integration (VLSI) layout is encapsulated into an abstract logic representation are often considered untrusted [9].

5.2 CAD Tools for Modification of RTL

CAD tools can be periled appositely tapping software vulnerabilities to alter RTL [10] without the intercession and intent of the designer and once compromised, it would be a herculean task to detect. Besides, the concept of SoC based on recyclable hardware is a permeating praxis in the semiconductor industry today owing to the huge diminution in cost and time attributes involved. Sadly here, only the supply and demand factors are being addressed, i.e., the user is only interested in getting his functionalities right and the seller may just be involved to ensure the same reaches the customer at the right time but the malicious untrusted third party in the process may butt in something unknown to either that can be a reason for chaos later.

5.3 Malicious Reprogramming of FPGA

A typical customer holds a bare manufactured IC and configures the same with the help of a field-programmable gate array. The FPGA configuration is generally specified using a hardware description language (HDL), similar to that used for an application-specific integrated circuit (ASIC).

5.4 Side-Channel Attacks

MOLES [11] aka Malicious Off-chip Leakage enabled by Side channels engineered to leak information below the effective noise power level of the device. Vital and critical data vide Moles can be retrieved with the assistance of spread spectrum technology, i.e., a type of wireless communications in which the frequency of the transmitted signal is designedly altered [12] and since the signal of the reduced information vanishes in the noise, it becomes arduous of what data has been transferred [13]. HT based on this actually is a novel way to designedly leak out information.

5.5 Malicious Processor

n advantageously contrived and implanted backdoor at an untrusted fabrication facility involved in manufacturing the typical pc processor can be victimized by a software antagonist at a later scheduled timeline. Such backdoors are ordinarily designed to be out of action during booting or activated under uncommon predetermined stipulates or can get activated with a singular rare input condition that is

ascertained by the malevolent intender [14]. This kind of a backdoor in a processor will never be divulged by the run of the mill or state of the art antivirus versions predominately available COTS.

6 Known Cases of HT in Recent Times

It comes as a surprise though that such a severe threat that is currently the topic of various forums, discussions, conferences, and research work has no such case studies to know the impact. Whatever heard and read is all discredited and only suspected, for e.g., Operation Orchard [15] wherein a Syrian nuclear reactor was subjected to Israeli Airstrike, seems to have been worked out via a hidden kill-switch function in the radar infrastructure. This functionality was then thought to be used to disable the Syrian radars for the short duration of the attack.

Mi-grade FPGA chips, e.g., ACTEL have been a suspect of containing a backdoor function that's equivalent of admin debug designed into the JTAG functionality of the subject chip IC. The subject IC Actel/Microsemi ProASIC3 chips could be used for accessing FPGA configuration using this backdoor. The researchers confirmed that this backdoor was not present in the original firmware loaded with the chip [16].

7 Measures to Detect Hardware Trojans

Vide above basic introduction we can see the kind of potent threat this brings along and the worst part till date is no formal or assured methods exist to detect any such threats. A typical hardware Trojan threat can actually exist in an IC as a 5–6 line code that gets activated under predefined conditions as a set. Though at present the severity of the threat being realized is finally forcing IT security domain to look and seek ways to resolve. Few good but only prelim measures include the following.

7.1 Embedded Systems Challenge

Polytechnic Institute of New York University based at USA every year organizes this competition by the name of Embedded Security Challenge (ESC) that bids two teams in a contest wherein one team designs target system hardware and the other team tries to identify and exploit the vulnerabilities in the target hardware [17].

7.2 Trust in ICs

This concept aims at a secure cycle of IC design and manufacturing primarily comprehending insertion points including chip authentication, IC design, IP protection, and manufacture [18]. Defense Advanced Research Project Agency backs the SHIELD [19] (Supply Chain Hardware Integrity for Electronics Defense) program that proposes to build trust in the typical supply chain that involves Design, Manufacturing, Testing, Integration, packaging, and finally distribution. The SHIELD root of trust as proposed would be able to avow the provenance of an IC as it goes through the typical Supply chain processes.

7.3 Golden Model Fabrication

One way of ensuring a Hardware Trojan free IC is a fabrication of the complete IC in a trusted plant with no third parties involved and no outsourcing involved. Once fabricated, this IC can be used as a reference model for "Integrated Circuits under Test" for behavioral and performance deviations [20].

8 Countermeasures to Detect Hardware Trojans

Probably, as we see above, these are only too prelim measures to counter Hardware Trojans perhaps a long way to go before a 100% trusted IC checks in before us. Ideally any malevolent modification to any IC should be perceptible during tests and inspections whilst pre-silicon manufacturing or post-silicon testing but that is not an easy thing to do since the complex ICs today, with so many multiple agencies involved at various echelons of manufacturing and design, will unlikely have a golden model of the intact IC. Moreover, if the antagonist decides to taint only a minuscule percentage of the complete batch of ICs being manufactured, the complexness to detect only step-ups further. Another way out for detection involves Nanometer physical inspection [21] which is for one very complex from point of conduct but also is mostly not economically viable. Vide [22], the countermeasures for HT as concentrate on three panoptic categories of countermeasures for protection against HT. These include Runtime monitoring, Design for security and Trojan Detection approaches which attempt to arrest any kind of malicious embedding of HT at prefabrication stages using pre-silicon test approaches or using non destructive techniques at post-silicon manufacturing test stage. The Run *Time Monitoring* approach is based on online monitoring while the circuit is in operation. The *Design for Security* approach essays to make the insertion of HT at any stage hard or facilitate detection ease during pre/post fabrication whereas the *Trojan Detection* approach can be logic testing based on generating set and predefined test

patterns and side-channel analysis for HT. Between these, *Design for Security* approach may not be a very effective way to resolve the HT threat owing to the diversity of threat classification discussed above whilst *Runtime Monitoring* may be more effective since this approach can be applied for real-time monitoring.

8.1 Destructive Versus Nondestructive Detection Technique

Once the IC is fabricated and boxing concluded for use by the end user, there remains very restricted ambit and visibility to endeavor to detect any kind of HT presence. However, destructive reverse engineering resolves to an extent in such cases. It involves depackaging the IC, acquiring microscopic images of each layer, trust validating the same after rebuilding the design of the end product. This approach uses a sample of the infected batch of ICs, thus it would be judicious to apply this wherein infection or insertion of the HT is limited to a small percentage. Scanning Electron Microscopy (SEM) is used to destructively delayer one chip wherein all of the transistors and connections can be averred. Also, this approach makes the IC under test unusable further, that's why the name destructive came to the fore. It takes from weeks to maybe months depending upon the complexity of the IC under detection for giving a 100% assurance of an HT free IC. Nondestructive methods relate to ways of detection that keeps the chip usable after the test. Between the two, Destructive detection technique is more effective viz-a-viz nondestructive detection technique.

8.2 Homomorphic Encryption/Decryption

One of the countermeasures against Hardware Trojans proposed by Aliyu and Bello [23] is the use of Homomorphic Encryption and Decryption which offers brilliant security boasts since it allows operating on data without revealing the contents being worked at. Homomorphic encryption is a type of encryption which allows processing of data on ciphertext and generates an encrypted result which on decryption is valued equally to the one processed with plain text. This certainly is an advantage plus for handling Hardware Trojans. Homomorphic encryption may be Partial or Full where Partial Homomorphic proffers to do either multiplication or addition on ciphertexts without unwrapping the original plaintext data while Full Homomorphic appropriates efficacious rating of a capricious depth circuit compiled of multiplications and additions.

9 Conclusion

IC is the basic core component of the diverse range of electronic systems being exploited across various domains pan globe today and the growing dependence makes it essential to ensure these ICs faithfully and sincerely perform the tasks they are designed and fabricated for. Hardware Trojans being inserted or retrofitted at any stage in these ICs are thus a grave threat that stands as a serious challenge today for the IT security domain. The software industry which has been campaigning in all gears put into ascertaining a malware/virus free application or an OS, over decades now, is yet to reach anywhere as daily various zero days keep getting deciphered which might be existing in an unknown quantified figure. The HT threat actually adds to the excruciation since this is indeed indecipherable with the present set of researches and studies did across. The future researches have a wide domain to work on starting to explore the emerging attacks on these ICs, developing trust validation standards for ICs being manufactured in the electronic industry and come out with inexpugnable apt approaches to counter such threats.

References

1. Trojan at https://en.wikipedia.org/wiki/Trojan_horse_%28computing%29
2. Mitra S, Wong HSP, Wong S (2015) Stopping Hardware Trojans in their tracks
3. Bhunia S (2014) Hardware trojan attacks: threat analaysis and counter measures
4. Karri R (2010) Trustworthy hardware: Identifying and classifying Hardware Trojans. IEEE Comput 43(10)
5. Wang X, Plusquellic J (2008) Detecting malicious inclusions in secure hardware: challenges and solutions. In: Proceedings of the 2008 IEEE international workshop on hardware-oriented security and trust, Washington
6. Zhang J (2014) DeTrust- defeating hardware trust verification with stealthy implicitly-triggered Hardware Trojans
7. Shield J, Hopkins B (2015) Hardware Trojans—a systemic threat
8. Shield J, Hopkins B (2015) Hardware Trojans—a systemic threat, p 47, Para 5
9. Shield J, Hopkins B (2015) Hardware Trojans—a systemic threat, p 49, Para 5.3
10. Aliyu A, Bello A (2014) Hardware Trojan model for attack and detection techniques
11. Rad R, Plusquellic J, Tehranipoor M (2010) A sensitivity analysis of power signal methods for detecting Hardware Trojans under real process and environmental conditions
12. Wu TF, Wong HSP, Wong S, Mitra S (2015) TPAD-hardware trojan prevention and detection for trusted integrated circuits
13. Lin L, Burleson W (2009) MOLES—malicious off-chip leakage enabled by side-channels
14. Spread Spectrum at http://searchnetworking.techtarget.com/definition/spread-spectrum
15. Hardware Malware book By Edgar Weippl (2013) Adrian Dabrowski, Heidelinde Hobel, p 67, para 4.2
16. King ST, Tucek J, Cozzie A, Grier C, Jiang W, Zhou Y (2008) Designing and implementing malicious hardware. In: Proceedings of the first USENIX workshop on large-scale exploits and emergent threats(LEET)
17. Adee S (2008) The hunt for the kill switch. IEEE Spect 45(5):34–39

18. Skorobogatov S (2012) Breakthrough silicon scanning discovers backdoor in military chip. In: Cryptographic hardware and embedded systems (CHES'12), vol 7428. Springer, Berlin, pp 23–40
19. The Embedded Systems Challenge at https://csaw.engineering.nyu.edu/
20. DARPA Trust in IC at http://www.darpa.mil/program/trusted-integrated-circuits
21. Shahrjerdi D, Rajendran J (2014) Shielding and securing integrated circuits with sensors
22. Hardware Malware book By Edgar Weippl (2013) Christian Krieg, Adrian Dabrowski, Heidelinde Hobel, p 67, para 4.2
23. Aliyu A, Bello A (2014) Hardware Trojan model for attack and detection techniques

Author Biographies

Anupam Tiwari is an IT Security enthusiast and an incisive learner, holds rich experience and qualifications in the demesne including CDAC & GFSU Certified Cyber Security Professional, Certified Ethical Hacker with B.E and M.Tech in Computer Science from JNTU Hyderabad. He also holds three post graduation qualifications in Information Security, ERP and Operations & Systems and presently pursuing his research in the world of cryptocurrencies. He is a senior member and regular contributor to articles in leading defence and engineering journals. He has been a regular participant in National and International Seminars as a guest speaker and He is working with the Min of Defence wherein he has variegated experience of service in IT security implementations and conduct of Cyber Audits.

Chetan Soni is an cyber security follower. He holds vast experience and qualifications in field of cyber security. He is B.E. in computer science and holds two PG Diploma in field of Information security and Aeronautical engineering. He has done various certifications in field of Information Security including CEH. He has ten years of experience in domain of Information Security. His area of interest is implementation of firewalls and network security. He is presently working with Min of Defence where he has implemented various cyber security measures and conducted Information Security audits in his organization.