THE ANNALS OF “DUNĂREA DE JOS” UNIVERSITY OF GALATI
FASCICLE III, 2020, VOL. 43, NO.3, ISSN 2344-4738
ELECTROTECHNICS, ELECTRONICS, AUTOMATIC CONTROL, INFORMATICS
Article DOI: https://doi.org/10.35219/eeaci.2020.3.02

CLASSIFICATION OVERVIEW OF THE HARDWARE TROJANS IN DIGITAL CIRCUITS

Grigore Mihai TIMIS*. Alexandru VALACHI.*

**Technical University “Gh.Asachi”Iasi, Faculty of Automatic Control and Computer Engineering (e-mail: mtimis@ tuiasi.ro, avalachi@tuiasi.ro).*

Abstract: This paper presents an overview of the Hardware Trojans classification methods. A malicious entity can introduce a Hardware Trojan (HT) into a design in order to denial of service, destroy or disable the system. Moreover, it could leak the confidential information and the secret keys before altered them. The Hardware Trojan (HT) threats should be analyzed with maximum importance through the entire lifecycle of the integrated circuit (ICs). A hardware protection against the detected harmful logic should also be implemented.

Keywords: Hardware Trojan detection, Hardware Trojan prevention, Hardware Trojan attacks, Hardware Trojan classification, Hardware Trojan Taxonomy.

1. INTRODUCTION

One of the most actually problem faced up by the design engineers on the integrated circuit (IC) chips is represented the trust and the security of the digital circuits. Globalization in the integrated circuits industry decreases the control of the System on Chip (SoC). Adding of the 3rd party Intellectual Properties (IPs), design tools, outsourcing fabrication, this will lead to a lower cost and meet the time to market targets, (Wang, 2008), (Tehranipoor et al., 2011). Thus, using a 3rd party IP cores known as black boxes, instead of building these blocks from the scratch, it can contain Hardware Trojans (HTs) which could generate potentially malfunction of the SoC normal functionality. The type of the malfunctions can be denial of service attack (DoS) and cause privacy leakage. These Trojans must be detected in the pre-silicon phase, otherwise it can infect millions of ICs through a Trojan affected IP core, (Wang et al., 2008), (Karri et al., 2010), (Karri et al., 2011), (Jin et al., 2009), (Hu et al., 2017), (Palanichamy et al., 2016).

Hardware Trojans (HT) are modifications of the original circuit, inserted by an unintended entity in order to exploit and to gain access to data or software running on chips, (Bhunia et al., 2014), (Kumar et al., 2015), (Jacob et al., 2014).

Based of the Intellectual Properties (IP) reasons, the IP core vendors does not offer the RTL source code of the IP core. Thus, the digital IP cores are generally offered in the netlist format which consists of the common digital logic gates and memory elements.

Even if the RTL source code of the IP core is available, it could be not so feasible in case of large IP's cores to manually inspect the source code for the Hardware Trojans.

These vulnerabilities have raised concerns regarding the possible threats to the financial infrastructures, military systems, transportation security etc. (Flottes et al., 2015).

A malicious entity can introduce a Hardware Trojan into a design in order to denial of service, destroy or disable the system. Moreover, it could leak the confidential information and the secret keys before altered them, (Exurville et al., 2015), (Rajendran et al., 2014).

Trojans can be implemented as hardware changes to ASICs, microprocessors, digital signal processors (DSPs), microcontrollers, different kind of processors and logic. They can be also implemented as firmware modifications – FPGA bitstreams, (Kumar et al., 2015).

According with (Karri et al., 2010), (Jacob et al., 2014) an IC fabrication process contains three major steps: designs, fabrications and manufacturing. Thus, also the fabrication and manufacturing steps might be considered untrusted since an attacker can substitute Trojan ICs for genuine ones.

There are two main directions in order to ensure that a chip used by a client is authentic, (Wang et al., 2008), (Bhunia et al., 2014), means that it only respects the full functionalities described by the documentation and nothing more.

The first option is to ensure that the entire fabrication process is securely and trusted.

The second option is to check the trustworthiness of the manufactured chips upon return to the client. This step is known as silicon design authentication.

In general, the hardware based security techniques, (Xie et al., 2016), (Jacob et al., 2014) modify the hardware in order to prevent possible attacks and to protect IP blocks or secret keys. It's considering that an unintended person-attacker, will alter the design before or during the fabrication.

As specific literature (Tehranipoor al., 2011), (Ursaru et al., 2009), (Hu et al., 2017), (Bhunia et al., 2014), (Alkabani et al., 2008) relates, the 3rd Hardware Trojans (HT) circuits are usually activated during a specific or couple of specific conditions are meet: e.g. sensing a specific design signal which can be as temperatures, power or an output value of a specific logic is activated.

Hardware Trojans (HT) detection is still a new research area, but it has accounted a significant attention in the past decade, (Palanichamy et al., 2016), (Xie et al., 2016), (Jacob et al., 2014).

This paper presents the current state of knowledge on existing detection schemes and design methodologies for improving HT detection methods.

The detailed outline of the paper: Section II, Hardware Trojan design and taxonomy; Section III, Insertion of a Hardware Trojan Horse (HTH); Section IV, Conclusions and Further work.

2. HARDWARE TROJAN DESIGN AND TAXONOMY

The first detailed taxonomy for Hardware Trojans was developed by (Wang et al., 2008), (Tehranipoor et al., 2010).

The taxonomy showed in Fig.1 lets researchers to choose their Trojan detection techniques methods. Because malicious alternations to a chip's structure and function can take many forms, (Wang et al., 2008) the Trojan taxonomy is decomposed into three main categories:

- physical characteristics
- activation characteristics
- action characteristics

According with Fig.1, the physical characteristics show the Hardware Trojans (HT) behaviour. The Type category splits (HT) into functional and parametric classes. The Functional class include trojans that are physically realized through add/remove of logic gates.

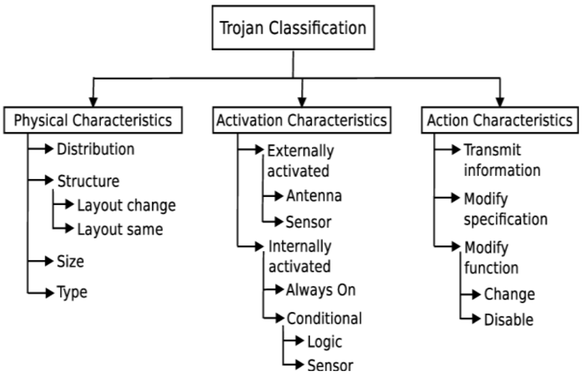

Fig.1. Hardware Trojans taxonomy (sources: (Tehranipoor et al., 2010), (Wang et al., 2008))

The activation characteristics represent the mode when the HT becomes active and are able to produce destructive function effects. It can be externally activated (e.g. by a sensor) and internally activated, upon a condition is meet.

The "Always on" means that the HT is always active and can corrupt the chip's behaviour at any moment in time.

Action characteristics identify the types of destructive behaviour introduced by the HT. The modify function class refers to HT that can change the chip's behaviour by adding logic, removing or bypassing the logic.

3. INSERTION OF AN HARDWARE TROJAN HORSE (HTH)

According with Fig. 2, (Tehranipoor et al., 2010), Hardware Trojan Horse (HTH) insertions can be classified into four categories:

- internal trigger
- external trigger
- HTH storage

- HTH driver

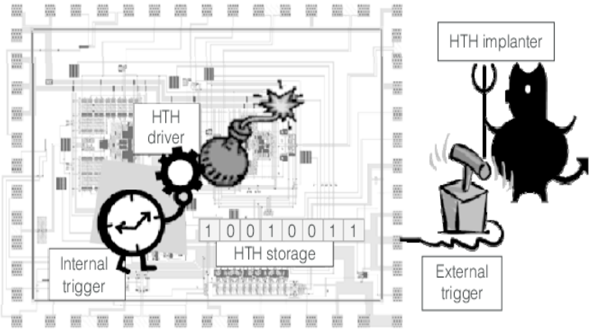

Fig.2. Hardware Trojan Horse (HTH) components (source: (Tehranipoor et al., 2010))

Trigger can be associated with an external/internal event or a predefined value of a bus/signal.

After the trigger is activated, the action to be taken can be stored in a sequential circuit or in a memory.

The actions implementation of the trigger is executed by the driver.

Fig. 2 presents an overview of the Hardware Trojan Horse insertions into an Integrated Circuit (IC) using a presynthesis manipulation of the circuit's structure.

This kind of approach represents the issue of trust in IP cores designed by a 3rd party vendor(s).

Fig. 3 presents an overview of the design process.

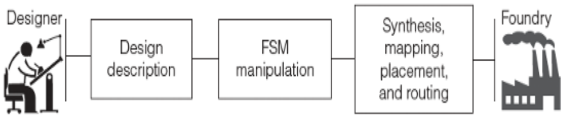

Fig.3. HTH can be inserted during design process (source: (Tehranipoor et al., 2010))

The finite state machine (FSM) can represent the computation model of the circuit.

By altering the FSM as embedding new states, a Hardware Trojan Horse can be inserted in the circuit.

The modified FSM should have a trigger as an input and driver which is hidden into the FSM structure.

In this way, the HTH is un-removable from the original design behavior.

The HTH embedding model provides a low-level mechanism for bypassing higher-level authentication models.

There are cases when a HTH can pass a functional test through bypassing the state-of-art detection methodologies.

In combinational logic systems, by adding malicious logic, the output signal value can be altered when (HT) triggering condition is fulfiled.

In the paper (King et all., 2008), considering the several attacks, it designed and implemented the Illinois Malicious Processor with a modified CPU. Thus a malware firmware was executed using stealthy execution. The attack was evaluated using a FPGA evaluation development board by changes the VHDL code of a Sparc V8 processor that includes a MMU (Memory Management Unit).

The additional timing overhead compared with the original version is approx. 12%, while in the logic is about 1%, (King et al., 2008).

Three potential attacks were implemented as:

- privilege escalation attack
- a log-in backdoor in shadow mode
- a password stealing service which is sending to the attacker

In conclusion, (King et al., 2008) affirms that the hardware is practical and could support various attacks, while is not so easy to detect.

Another method consists by insertion of the malicious circuit into the design using the mechanism for actively IC controlling, for example the IP core.

For example, altering the finite state's machine that cannot be reverse-engineered, it could be used to embed (HT) circuits by handling mechanism in order to remotely controlling, activating and disabling the hardware Trojan (HT).

4. CONCLUSIONS AND FUTURE WORK

The Hardware Trojan (HT) issue has become a more and more sensitive security concern for a design service nowdays, thus the detection of them becomes a very challenging problem.

Based on the diversity of the Hardware Trojans types, one unique method cannot be reliable for all of them, thus why a 100% detectability seems to be impossible.

HT is designed to avoid detection since they run in stealth mode. There are widen methods regarding the triggering modes which avoid the IC's testing procedures (e.g. different combinations of the primary inputs).

One of the used method that help HT detection is based on logic testing where the goal is to remove low controllable signals in order to prevent the creation of a stealthy condition, (Tehranipoor et al., 2011), (Flottes et al., 2015). This kind of method will be detailed on a future research paper.

The methods of how to insert a Hardware Trojan in a digital circuit and how it can be detected by a targeted attack will be discussed on a future research paper.

5. REFERENCES

Mohammad Tehranipoor and Farinaz Koushanfar, "A survey of hardware trojan taxonomy and detection", IEEE Design & Test of Computer, 27:10-25, 2010.

S. T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, and Y. Zhou, "Designing and implementing malicious hardware," in Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, ser. LEET'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 5:1–5:8.

Y. Alkabani and F. Koushanfar, "Extended Abstract: Designer's Hardware Trojan Horse", Proc. IEEE Int'l Workshop Hardware-Oriented Security and Trust (HOST 08), pp. 82-83, 2008.

Wang, "Hardware Trojan Detection and Isolation Using Current Integration and Localized Current Analysis", Proc. IEEE Int'l Symp. Defect and Fault Tolerance of VLSI Systems (DFT 08), pp. 87-95, 2008.

M Tehranipoor, H. Salmani, X. Zhang, X. Wang, R. Karri, J. Rajendran and K. Rosenfeld, "Trustworthy Hardware: Trojan Detection and Design-for-Trust Challenges", In IEEE Computer, pp. 66–74, 2011.

Wang, M. Tehranipoor and J. Plusquellic, "Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions", Proc. IEEE Int'l Workshop Hardware-Oriented Security and Trust (HOST 08), pp. 15-19, 2008.

R. Karri, J. Rajendran, K. Rosenfeld and M. Tehranipoor, "Trustworthy Hardware: Identifying and Classifying Hardware Trojans", In IEEE Computer, pp. 39–46, 2010.

Y. Jin, N. Kupp and Y. Makris, "Experiences in Hardware Trojan Design and Implementation", Proc. IEEE Int'l Workshop Hardware-Oriented Security and Trust (HOST 09), pp. 50-57, 2009.

W. Hu, L. Zhang, A. Ardeshiricham, J. Blackstone, B. Hou, Y. Tai, et al., "Why you should care about don't cares: Exploiting internal don't care conditions for hardware Trojans", pp. 707-713, 2017.

S. Bhunia, M. S. Hsiao, M. Banga and S. Narasimhan, "Hardware trojan attacks: threat analysis and countermeasures", Proceedings of the IEEE, vol. 102, no. 8, pp. 1229-1247, 2014.

K. S. Kumar, R. Chanamala, S. R. Sahoo and Mahapatra, "An improved AES Hardware Trojan benchmark to validate Trojan detection schemes in an ASIC design flow", International Symposium on Vlsi Design and Test IEEE, pp. 1-6, 2015.

ML Flottes, S Dupuis, PS Ba and abd B Rouzeyre, "On the limitations of logic testing for detecting Hardware Trojans Horses", International Conference on Design & Technology of Integrated Systems in Nanoscale Era IEEE, pp. 1-5, 2015.

I. Exurville, L. Zussa, J.B. Rigaud and B. Robisson, "Resilient Hardware Trojans Detection based on Path Delay Measurement", In International Symposium on Hardware-Oriented Security and Trust (HOST'15), pp. 151–156, 2015.

J. Rajendran, O. Sinanoglu and R. Karri, "Regaining Trust in VLSI Design: Design-for-Trust Techniques", In Proceedings of the IEEE, Special Issue on Trustworthy Hardware, 102(8):1266–1282, 2014.

Ovidiu Ursaru, Cristian Aghion, Mihai Lucanu, Liviu Tigaeru, "Pulse width Modulation Command Systems Used for the Optimization of Three Phase Inverters", Advances in Electrical and Computer Engineering Journal. Suceava, Romania, 2009, pag.22-27.

M. Palanichamy, P.S. Ba, S. Dupuis, M.L. FLottes, G. Di Natale and B. Rouzeyre, "Duplication-based Concurrent Detection of Hardware Trojans in Integrated Circuits", In Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE'16), 2016.

Y. Xie and A. Srivastava, "Mitigating SAT Attack on Logic Locking", In Conference on Cryptographic Hardware and Embedded Systems (CHES'16), pp. 127–146, 2016.

N. Jacob, D. Merli, J. Heiszl and G. Sigl, "Hardware Trojans: current challenges and approaches", in IET Computers & Digital Techniques, 8(6): 264 – 273, 2014.