Addressing Hardware Security Challenges in Internet of Things: Recent Trends and Possible Solutions

Subha Koley, Prasun Ghosal
Department of Information Technology
Indian Institute of Engineering Science and Technology, Shibpur
Howrah 711103, WB, India
E-mail: {subhakoley, p_ghosal}@it.iiests.ac.in

***Abstract*—Internet of Things (IoT) is an emerging technology where each and every 'thing' is possible to be connected through a network and also controllable from any remote station. Coming few years, IoT is going to be an unavoidable part of our daily lives. Every sector like manufacturing farms, traffic controls, real-time environment monitoring, security systems, health-care, e-agriculture etc. is going to be governed by IoT as backbone. Ensuring security during this voluminous information exchange becomes a critical issue in this context. It applies equally to both device communication, control signals, and information exchange. In this paper an approach has been made to identify major security and privacy flaws existing in IoT enabled devices especially from hardware perspectives, and thereby to present possible solutions to existing challenges for conversion of 'Internet of Things' in 'Internet of Secure Things'.**

***Index Terms*—Internet of Things; Security; Privacy; Hardware Trojan.**

I. Introduction

In this present era Internet of Things (IoT) is one of the most emerging and developing technologies in communication centric computing perspective. The vision of IoT is to interconnect all the devices in the planet with existing Internet infrastructure and thereby utilize the enormous capability of internetworked knowledge base during their operations.

The phrase 'IoT' is constructed with two very important words viz. 'Internet' and 'Things'. From Internet perspective, IoT needs such a network that is available everywhere and every time (anytime, anywhere) i.e. ubiquitous network [1]. 'Things' in IoT could be any item that is uniquely identifiable. Not only our traditional computers or cell phones but the sensors, actuators, RFID tagged elements, everything could act as a 'thing' in IoT enabled systems [2]. It is expected that in 2020 there will be more than 50 billion 'things' connected to IoT [3]. 128 bit IPv6 protocol gives us the opportunity to assign ubiquitous ids to trillions of objects in the network [4]. These huge numbers of objects in the network brings us to a very difficult situation to manage the huge information-base securely. Privacy protection, confidentiality, access control etc. are very basic criteria any user can demand. But considering today's nano-scale computing, security and privacy preservation have become extremely challenging tasks. In present scenario, the security and privacy threats in distributed systems are not bounded in software level (network layer) only but hardware or physical layer security is increasingly becoming a growing headache towards the designers as well as researchers.

Overall organization of the rest of the article is as follows. Section II discusses about the present position of IoT security. Analysis and identification of key challenges in software as well as hardware level security issues are described in the succeeding section i.e. section III. A more detailed and focused analysis over hardware Trojans is presented in section IV. Analysis has been done and challenges have been identified to detect hardware Trojans and presented in section V. Some recently reported techniques as well as some possible approaches to mitigate this problem have been addressed in section VI. Finally section VII concludes the article with a note towards possible future directions.

II. Present Scenario

To start with some real example let us consider a smart home well equipped with smart security systems and close circuit television (CCTV) cameras everywhere. Let us imagine if someone manages to hack the security system or get the privilege to control the cameras or smart locks that would be the worst thing we could ever imagine. Or if somebody manages to get access our smart car's control? The situation gets worst when someone gets control of smart health-care system. In fact, when Mr. Dick Cheney (former vice president of USA) was hospitalized, the US security agency had disabled all wireless capabilities of the health monitors and smart apparatus to protect him [5].

"Without Trust and Security, Web Services are dead on arrival" — Phillip Hallam-Baker.

It is very clear that without proper security and privacy policies IoT could be the worst enemy of our daily lives. Recently HP has released a survey report [6] where it shows that there are 25 security flaws in IoT enabled devices. So it is very clear that the IoT systems are not at all well secured to adopt them in reality. The major challenges in privacy preservation and security of IoT is discussed in the next section.

978-1-4673-7211-4/15 $31.00 © 2015 IEEE
DOI 10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.105

III. Key Challenges in IoT Security

Any distributed system is expected to be well secured and reliable that can meet the clients' privacy criteria. And when the issues come to defense or medical sector, the security system is the first thing to be considered. IoT system has vast applications in sensitive government and personal lives. But we never can say that the environment is fully secure. The key challenges in IoT security are discussed here.

- Most of the IoT devices are extremely small in size. It is very hard to add extra security module to those tiny 'things'.
- Most of the 'things' have very low computational capabilities. So present complex security algorithms are not suitable for them.
- Limited power in IoT 'things' is the most challenging barrier to IoT security. Because of any extra security module, whether software or hardware, it needs extra energy to perform. But IoT systems, especially the wireless systems, are always expected to be energy efficient.
- The software of 'things', in most of the cases, can't be updated. So the present secure device may become insecure after few years.
- The industry hasn't taken the physical layer security issues seriously till now. But the hardware level threats are increasing exponentially in electronic devices.

The security issues can be divided in two major sections, viz. Software level threats, and Hardware level threats.

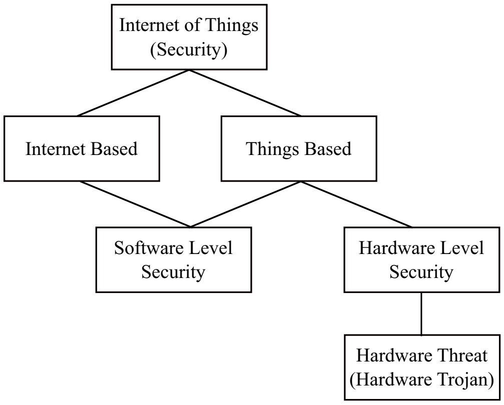

Fig. 1. Software and Hardware level security in IoT

A. Software level Security Issues

Hacking, information leakage, illegal access etc. come under this domain. Lack of proper security and privacy protection we can't dare to use those high-tech systems in our daily lives. It is possible to enter a malware to the system without users' knowledge, because most of them never force the system to malfunction. But they can collect our secret information like passwords and/or credit card information etc. and can send them to their boss. There is tendency to choose small and easy passwords for novice users. Most of the cases the hackers target them by brute-force attack to guess the passwords. Use of updated virus database, firewall, up-to-date software can protect us to some extent against these attacks. The encryption algorithms need to be stronger, less complex, and energy efficient so that the tiny devices in IoT can afford them. Software level security is a well-studied topic in information technology but what about hardware security? In Figure 1. we have shown software and hardware level security architecture in IoT enabled devices.

B. Hardware Level Security Issues

The security issues in IoT are not bounded within data authentication, access control, client privacy, and other attacks like data leakage. Hardware level insecurity is also grabbing the attention of researchers nowadays and it is becoming a growing problem day by day. To get a complete hardware secured IoT system, we need to secure the ICs (better to say NoCs [Network on Chip] or SoCs [System on Chip]) in the IoT enabled devices first. With tremendous growth in integration density with the ever increasing logical complexity of today's nano-scale electronic systems design and fabrication of VLSI chips have become a completely distributed system. Due to very high cost of fabrication process the IC (integrated circuit) designer companies need to depend on other vendors. This brings us to a comparatively insecure environment to design the IC's. Use of third party Intellectual Property (IP) core [7] and other design tools (CAD tools) make the situation more complicated. Because a single malicious circuit can be injected at any stage of the design process invisible to the designers at that time. Threats can also be injected during the running of a chip after successful fabrication. In first case that particular threats can run and force the IC to malfunction after the chip is fabricated and started working. As a result confidential information can be leaked or important instructions can malfunction. Hardware Trojan is one of them. In the next section we have discussed hardware Trojan in details.

IV. Hardware Trojan

Hardware Trojan is the malicious circuit or modification of the hardware of the IC during the design or fabrication process [8]. This results the malfunctioning of the IC during its runtime. In modern IC design process most of the stages are not secure well to detect this kind of threats due to its distributed nature. And most of the cases the Trojans are almost impossible to detect in the packaging and testing phages.

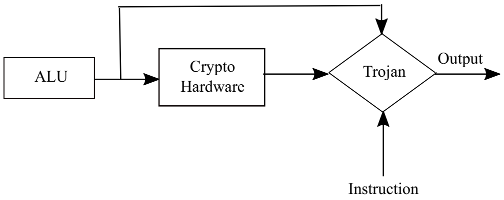

Fig. 2. Working Process of a Simple Hardware Trojan

The Trojan circuits can be injected at any phase of a VLSI design life cycle [9]. Specification, design, fabrication, and packaging are the most insecure phases, detected, when Trojans can be inserted. Hardware Trojan can be located at any component of a SoC. Processor, input output module, memory, power supply etc. everywhere they can reside. They can change in output of a system, damage a chip or leak secure information. In Figure. 2 a simple working process of a HT (Hardware Trojan) is shown. The authors of [10] classified Hardware Trojans based on their activation property as follows.

A. Always On

Some Trojans start working when the ICs begin working after fabrication. They are designed to work all the time. Basically their task is to monitor the activity of the chip and work accordingly. They can leak information, bypass instruction, control the whole chip, or damage the system. In IoT enabled systems the hackers can always monitor a system's activity using these types of Trojans.

B. Triggered

Most of the HTs remain inactive (sleeping mode) most of the times. But they become active at certain time. Trojans can be triggered internally or externally. Their working activity can be controlled by some predefined conditions embedded in it or from outside using the network. These types of Trojans get activated when they are required to perform.

1) Internally Triggered: Internally triggered Trojans start working when some specific condition of the chip occurs. The condition may be physical, logical, or timing. Actually they always monitor the conditions of the system and when the condition is met it triggers.

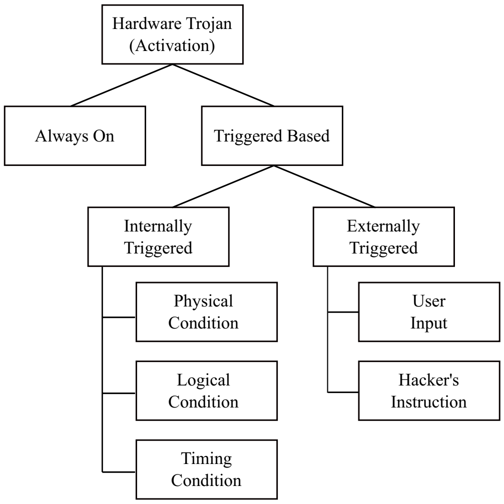

Fig. 3. Classification of Hardware Trojans

a) Physical Condition: The activation of these types of Trojans depends on the physical condition of the chip. The physical conditions can be temperature, pressure, stress, strain, or geographical location. For example, when the temperature of the system exceeds 50°C, the Trojan may start working. Or may be in a chemical farm when the pressure exceeds some predefined value, Trojan gets active to perform its work.

b) Logical Condition: Some Trojans become activated with some specific logical conditions. The conditions are usually predefined. They can be either combinational or sequential. They monitor the gate level conditions of the chip.

c) Timing Condition: These types of Trojans work as time bombs. Initially they are inactive, whatever the physical or logical conditions are. But after some predefined time, the Trojan starts working. They could be embedded with the system clock.

2) Externally Triggered: Some hardware Trojans are triggered externally. Not only the Trojan designers but the users can trigger Trojans unknowingly. Externally triggered Trojans are activated with some external inputs or instructions.

a) User Input: The user can enter some specific kind of input to the system that may activate the Trojan without user's knowledge. These Trojans only monitor the input signals to the chip and upon recognizing its activation signal they start performing.

b) Hacker's Instruction: When there is weak security in network layer, hackers can monitor or control the instructions of a NoC. They can activate the Trojan in the system externally by sending an instruction using the network.

In Figure 3, Trojan classifications are shown according to their activation property.

V. Challenges to Prevent Hardware Trojans

As evident from the above discussion, hardware Trojan is an emerging issue in electronics and computer application. All IoT systems are made of enormous SoCs that performs several private and confidential tasks. If there is a single hardware Trojan in any of the chips in the system, the security of the system may completely be destroyed. Let's find out what are the key challenges to prevent hardware Trojans.

- Nowadays ICs are designed in distributed environment. Due to high cost and extreme technological requirements, it is not possible to design and fabricate an IC by a single company. These distributed systems are not always well-secured to perform these kinds of sensitive tasks.
- Most of the ICs are multi-cores in nature and the cores are not always their own property. Usually they have to depend to third party companies for the IP cores. So it is not possible to verify them.
- The golden model [8] of the whole IC is not always available to one. So it is not possible to review the entire system to detect any mismatch in the circuitry.
- We use some CAD tools to design the chips, those are basically designed by others and we use them in the network. It is possible that there is software Trojans in the CAD that injects HTs automatically to the circuit model.
- Most of the cases the HTs are very small circuits made of few gates and transistors. It is very difficult to find out such a small circuit in the giant system.
- The Trojans are stealthy in nature. Most of them always remain inactive and activate only with some rare condition of the chip. So during testing phase it is almost impossible to detect them.
- HTs may be detected by de-packaging or reverse engineering process. But they are destructive in nature. And

as we don't have the golden model of the entire SoC, those processes are not worth it.

To get a completely hardware secure system, we first need to secure the environment and need to introduce some good policies to design the chips securely with preserving the third party company's privacies too.

VI. Some Trojan Detection Techniques

In spite of all of these unavoidable challenges, some Trojan detection techniques have been introduced by researchers. Some of them are discussed in this section.

A. *Current Integration Technique*

This technique measures the total current flow in each part of the IC [11]. If there is any Trojan present in the circuit, the flow must change at that particular section. But this measurement is a very sensitive task. Because most of the Trojans are very tiny in size and requires very minimum amount of current. Detection of this small current flow is really a tough task and requires very much sensitive apparatus. Also this process needs the golden model of the whole circuit to isolate the Trojan circuit.

B. *Path Delay Testing*

A Trojan, whether the size is, must cause some delay [12] in time taken by the IC. So, by calculating the delay amount we can identify some modification in the circuit. But this process needs high-dimensional path delay information of the original chip that may not be available all the time. Logically triggered Trojans activated with very rare case of logical conditions that may not occur at the testing phase. Also the path delay detection never guarantees presence of Trojan in the IC.

C. *Temperature Analysis*

If there is any extra circuit present in an IC that may generate some extra heat over the original one. In this approach we can measure the temperature generated by the chip and compare with the real one. But, the alteration of temperature can also be occurred by some other reasons. So a very accurate and well analyzed technique should be used.

D. *Power Based Analysis*

Any Trojan circuit must be connected with the power line to consume current, whether it is activated or not [13]. So we can compare the power consumption to detect any extra circuit in the chip. This technique can only detect the presence of a HT in the circuit but can't confirm the exact location of that. And as we have discussed earlier this measurement is very much sensitive in nature. Detection of this minute alteration in power consumption is a near impossible task and a challenging issue.

All these techniques are post-fabrication Trojan detection techniques and require the golden model of the whole SoC. Also these processes are very tough, sensitive, and never provide any guarantee of presence of Trojan in a system. There is no such technique available presently that we can say a 'silver-bullet' for hardware Trojan detection or prevention.

VII. Conclusion

Unfortunately the researchers have identified most of the security flaws in IoT enabled systems but there are no concrete solutions that can overcome all those problems at a time till date. To get a completely secure IoT enabled environment, we need to secure the 'things' from both, software as well as hardware levels. Software threats and hardware threats are dependent to each other. To secure the 'things' from hardware Trojans we have to overcome the challenges discussed in previous sections. It is very clear that within few years IoT is going to be an unavoidable part of our daily lives. So it's urgent to secure the IoT environment immediately before applying them in security and privacy sensitive applications.

References

[1] *"The Internet of Things"*, ITU Internet Reports, November, 2005.

[2] J. Gubby, R. Buyya, S. Marusic, and M. Palaniswami, *"Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions"*, Future Generation Computer Systems, Elsevier, Volume 29, Issue 7, September 2013, pp. 16451660.

[3] *"Internet of Things in 2020"*, INFSO D.4 Networked Enterprise & RFIDINFSO G.2 Micro & Nanosystems, in co-operation with the Working Group RFID of The ETP EPoSS, Version 1.1, May 27, 2008.

[4] K. Sakamura, *"Computers everywhere: The future of ubiquitous computing and networks"*, MIC Japan/ITU/UNU WSIS Thematic Meeting, *"Towards the realization of the ubiquitous network society"*, Tokyo, Japan, May 16-17, 2005.

[5] A. Grau, Illustration by J. D. King, *"Can You Trust Your Fridge?"*, IEEE Spectrum, March 2015, pp. 49-54.

[6] *"Internet of Things Research Study"*, HP Report, 2014.

[7] A. Das, G. Memik, J. Zambreno, and A. Choudhary, *"Detecting/Preventing Information Leakage on the Memory Bus due to Malicious Hardware"*, In Proceedings of Design Automation and Test in Europe (DATE), 2010.

[8] R. S. Chakraborty, S. Narasimhan and S. Bhunia, *"Hardware Trojan: Threats and Emerging Solutions"*, In proceedings of IEEE International High Level Design Validation and Test Workshop, 2009.

[9] N. A. Sherwani, *"Algorithms for VLSI Physical Design Automation"*, 3rd Edition, Kluwer Academic Publishers, 1999.

[10] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, *"Trustworthy Hardware: Identifying and Classifying Hardware Trojans"*, IEEE Computer Society, New York.

[11] X. Wang, H. Salmani, M. Tehranipoor, and Jim Plusquellic, *"Hardware Trojan Detection and Isolation Using Current Integration and Localized Current Analysis"*, In proceedings of IEEE International Symposium on *"Defect and Fault Tolerance of VLSI Systems"*, pp. 87-95, 2008.

[12] Y. Jin and Y. Makris, *"Hardware Trojan Detection Using Path Delay Fingerprint"*, In proceedings of IEEE International Workshop on Hardware-Oriented Security and Trust, pp. 51-57, 2008.

[13] M. Tehranipoor, H. Salmani, X. Zhang, X. Wang, R. Karri, J. Rajendran, and K. Rosenfeld, *"Hardware Trojan Detection Solutions and Design-for-Trust Challenges"*, IEEE Computer, pp. 64-72, 2011.