CSE 661 Term Paper, Fall 2016

# SECURITY AND PRIVACY IN INTERNET OF THINGS

RAJESH RAMESH
MS in COMPUTER ENGINEERING
SYRACUSE UNIVERSITY
416867192

***ABSTRACT*: The Internet of Things (IOT) has been emphasizing on interconnecting a lot of electronic devices in turn making them function automatically through simple instructions from users. It involves a lot of human-machine interaction. A variety of applications depend on this technology and therefore security and privacy are major issues. Each layer must have security principles so that secured IoT can be realized. Several countermeasures have been taken many researchers on each layer to enhance the security. At the same time, the electronic devices which are part of the system must be highly secured while transmitting signals since these devices are highly vulnerable to semantic attacks. Trust in communication entities and transferred data are of high importance. In this project, we review the hardware and software based security principles, challenges (mainly hardware), hardware Trojans, counter-measures, and prospects of securing IOT in the coming future.**

## I. I IoT AS THE NEXT EVOLUTION OF INTERNET – HOW IS IT CHANGING EVERYTHING

The Internet of Things (IoT), is bound to change everything around us—including ourselves. Looking at the impact of the Internet on science, business, government, education, communication, and humanity. Undoubtedly, the Internet has resulted to be one of the most important and powerful creations in human history. One can consider that Internet's next evolution is represented by IoT, as it takes a giant step in its potential to gather, analyze, and distribute specifics that can be turned by us into information and knowledge. Hence IoT becomes extremely important. A lot of IoT projects are underway in many sectors, which mainly aims at development. Also, it promises to close the gap between poor and rich by improving distribution of the world's resources to those who are in dire need of them, thereby helping us to understand our surroundings better and making us more proactive. As IoT is gradually growing, several roadblocks are coming up to threaten and impede the development of IoT, including the transition of address type to IPv6, having common standards, and developing enough energy materials for millions of minute sensors. However, IoT will continue to progress as many forces like tech-businesses, standards bodies, governments join hands to solve these challenges.

## II. IoT AS A NETWORK OF NETWORKS

Presently, the Internet of Things is made up of an unattached collection of dissimilar, purpose-specific built networks. For example, today's cars consist of various networks to safety features, control engine function, communications systems, and so on. Residential and commercial buildings are equipped with various multi-purpose control systems i.e., for heating, venting, and air conditioning (HVAC); security services; telephone services; and many others. As IoT gradually advances, all these networks that are related to it, will be well connected with added security, analytics, and management capabilities. This will allow IoT to become even more powerful in what it can help people achieve and will also allow the related applications to carry out operations in a more fortified manner.

## III. INTERNET OF HACKABLE THINGS – A MAJOR CONCERN

As many devices get connected to the Internet, the IoT system becomes more susceptible to attack, as new opportunities arise to exploit potential security vulnerabilities [3]. Currently time, cost and technical constraints challenge designers and manufacturers, thus allowing them to design these components with inadequate security features and creating potential security vulnerabilities. Such poorly designed and manufactured devices are bound to expose user-data to theft by leaving data streams unprotected. Also, IoT devices whose security levels are low, have the possibilities of allowing unauthorized dangerous users to change the configuration of those devices, hence causing them to malfunction. Thus, such unprotected become entry points for malicious cyberattacks.

Such attacks can be very much devastating in security-critical industries, such as the banks and military. Along with potential security design deficiencies, the sheer increase in the number and nature of IoT devices could increase the opportunities of attack. When coupled with the highly-interconnected nature of IoT devices, every poorly secured device that is “connected online potentially affects the security and resilience of the Internet globally, not just locally.

With huge advancements in technology especially in internet, humans are becoming heavily dependent on devices and systems that are internet-enabled and hence it difficult for them to function without such devices. Dependency on IoT devices for essential services are also increasing gradually due to increase in connectivity, hence it is a must for these devices to be designed with proper security principles.

With increase in dependence on IoT services, comes increase in the number of IoT devices, which give a good chance for malicious unauthorized users to gain access as many devices are bound to be released with inadequate security principles. It is always difficult handle a smart device than a normal internet-connected device like a tv, when under siege.

Therefore, IoT security with respect to devices and applications becomes a major discussion point and should be treated as a critical issue.

## IV. PRINCIPLES OF IoT SECURITY

Following are few hardware and software principles of IoT security that must be followed before planning to design and establish any IoT based system.

- Test for probability of scaling:

  The IoT system can consist of a large volume of devices. This implies that scaling of devices must be an important consideration in terms of design and security. Countermeasures for security can be carried out through scaling.

- Exploitation of Autonomy

  Though automated systems are designed to reduce human effort, they are very much capable of carrying out operations that are tedious, complex, and monotonous. Such operations are highly difficult for humans to understand and in most cases, they are ignored. Thus, IoT systems should find every opportunity to exploit this advantage for it to be secured.

- Provide Uniform Protection

  Data encryption in this context provides protection to those transmission paths that are used to transfer data. Though the data is basically unprotected i.e. before and after encryption. But when it is transmitted, it attains a good level of protection. There are few cases where the communication links do not have good security levels, hence leaving data unprotected. Consideration must be given to security of data in all aspects so that tampering is avoided. Encryption is not absolute -The metadata that conveys information regarding the encrypted data can be of good use to hackers.

- Harden the System as much as possible

  Make sure that the components of the IoT system are scaled and stripped down the smallest feasible feature that can the extent and surface of attacks. Disabling components like Unused ports and protocols, uninstalling all the unnecessary supporting software are few ways. Regular tracking of third party components should happen along with regular updating of these components.

- Supporting component lifecycle

  IoT systems must be capable enough to accommodate new components whenever necessary, especially in cases of emergency. Also, they should be able to accommodate existing components that are re-credentialed and must be able to remove existing components that have completed their full life cycle.

## V. IoT ATTACKS – AN INCIDENT – WHAT HAPPENED AND HOW IT DID HAPPEN

A fierce DDos attack was carried out on10/21/2016 against the website of Brian Krebs which forced him to remove his site after a few days [7]. The hackers carried out these attacks by directing lot of fake traffic at targeted servers, namely those belonging to Dyn, a major provider of DNS services. This affected the operation of major websites like Github, Verizon, Paypal, Tumblr, Spotify, Comcast, Reddit and Twitter. This incident also affected many online retailers due to which their retail operations were operations were interrupted and huge confusion was caused.

A large number of devices that are connected to the internet such as surveillance cameras and routers were insecure at that point of time and hence made it possible for such an attack to place. Malicious code was programmed by the hackers into such unprotected devices so that they could form a botnet. The software used by them stealthily moved within the internet to identify those devices that were unsecured and freely available. A large number of such devices were attacked at once and hence were capable enough to generate huge amounts of traffic that was bogus and ultimately directed them to the targeted servers.

Infections enabled by this DDoS attack were present due to the availability of default passwords and these passwords for most of the unsecured devices were widely known. Due to this issue, placing a device that in the internet without changing its default password can easily enable such attacks without anyone's knowledge. Recent surveys reveal that at least 15% of the home routers do not have enough security. This is shows that millions of home routers are unsecured and are highly susceptible to such malicious attacks in the near future.

## VI. IMPORTANT SECURITY CHALLENGES

Security of distributed systems is of utmost importance since they cater a large number of clients. They must be able to handle attacks well and must not succumb to them since privacy of data is the first thing any client will require in such systems. Looking at different sectors like military, government, medical, etc., security and reliability of systems is very much required since they consist of applications which are related to personal lives. Unfortunately, no system is fully secured. Following are the complex challenges that are faced in securing IoT:

•Though many IoT devices are quite energy efficient, there are few devices that get drained after a point of time. Providing such devices with additional modules for security, be it hardware or software, will be difficult since they will be required more energy to run these modules.

• It is extremely difficult to regularly update software for security. A device running on a software that is currently secure, can become insecure after a point of time due to this problem. Time constraints and volume of devices aggravate the problem.

• It is extremely difficult to provide additional modules to most of the devices since they are very small thus making them more vulnerable.

• Algorithms for security have been improving rapidly with time. The current security algorithms will be difficult to be implemented in most of the devices since their computational and processing capabilities are low. It is difficult to design them in a way that can allow the security algorithms to be processed easily.

• Attacks on hardware levels of devices have been greatly increasing. Unfortunately, more importance on security has been given only to the Application layer and the Network layer.

Thus, the threats to security can be broadly classified into Hardware Level threats and Software level threats.

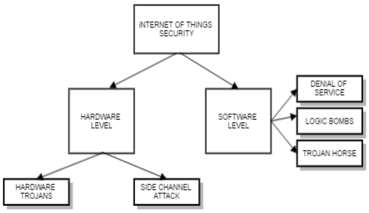

Figure 1: Classification of IoT Security threats

### A. HARDWARE LEVEL THREATS

When one discusses about security issues, the first thing that comes to mind is about data security and privacy and attacks related to it like malicious unauthorized access, leakage of data, etc. Insecurity with respect to Hardware is becoming a bigger concern since hardware level countermeasures are lesser when compared to that of software. Not much attention has been given to hardware, since security of data was prioritized. Security at hardware level is currently gaining more importance and attention. Integrated chips, Network on chips, System on chips need to be well secured so that one can achieve an IoT system that is completely secure in the hardware level. The current trend of designing and fabrication of VLSI chips has changed. It has become more of a distributed system since there is a lot of growth in the density of integration and the system design of Nano-electric systems has become even more complex. This leads to increase in fabrication costs due to which other designers pass on the responsibility to other vendors in the business. The design and fabrication and fabrication environments can be entirely different with respect to security in this case. Adding to the trouble and complexity are the usage of different design tools and third party intellectual property cores. The chip that is getting fabricated can undergo dangerous changes at any stage. One can inject a malign circuit into the chip at any stage and this will not be known to the designers.

During test runs after fabrication, one can inject threats into the chip, thus causing it to malfunction after fabrication. This can prove very dangerous to the ones who purchase systems with such damaged chips because there are high chances of confidential information leakage. Examples of such threats are Hardware Trojans and Side Channel Attacks

### B. SOFTWARE LEVEL THREATS

Unauthorized access, Hacking, leakage of information are the few threats that can occur at the software level. Systems that are highly systematic are not properly protected and have poor security measures. Such systems cannot be used even though they are helpful in carrying out complex operations. A malware can be easily inserted into an unprotected system without the knowledge of the user. Such malware do not cause damage to the operations of the system but can easily obtain confidential information of the user like stored passwords, credit card information, etc. When collected, this information can easily be misused. Amateur users generally set easily guessable passwords for their systems. The hackers use this as a chance and target them using a brute force attack that will help in guessing the passwords. Measures like updating the firewall, updating the virus-database and using up-to-date software can assist in keeping the system protected to an extent. Developing stronger encryption algorithms that are energy efficient, less complex, easy to compute and process can help in securing IoT devices.

In this paper, our discussion will focus only on Hardware Level Threats.

## VII HARDWARE TROJANS

Hardware Trojans are those malicious modifications that are made on the original chip designs that corrupt the chip's normal operation [1].

Techniques such as chemical mechanical polishing [1], path delay testing, temperature analysis, etc., are used to detect these Hardware Trojans. Since design and fabrication takes place in a distributed model, the entire process is divided into many stages where most of the stages do not have enough security measures to detect hardware threats. Trojans are those kind of threats that are impossible or almost impossible to be detected during the processes of packaging and testing. Few points where a Hardware Trojan can be located are, input /output modules, any component of a SoC processor, power supply etc. They can hide in miniscule points and are also capable of changing a system's output during it's operation, damaging a chip and leaking confidential information. Figure. 2 illustrates a simple working process of a Hardware Trojan.

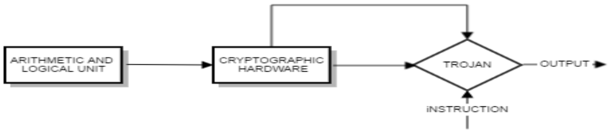

Figure 2: Working process of a Hardware Trojan

Hardware Trojans can be broadly classified into two types – Active/Always On and Triggered [4].

Always On Hardware Trojans: These Trojans start being active once the chip is fabricated and ready to use. They are designed to be active all the time. They keep monitoring the activities and operations of the chips and collect confidential information stored in them. They are capable of bypassing instructions and controlling the chip, ultimately damaging them. It is quite difficult identify such a Trojan unless an abnormal activity takes place. This Trojan enables the hackers to monitor the activities of the affected chips.

Triggered: They are not active all the time and are designated to function only at certain points of time. They do not start functioning unless they are triggered and this triggering can happen internally or externally. The triggering is classified as follows:

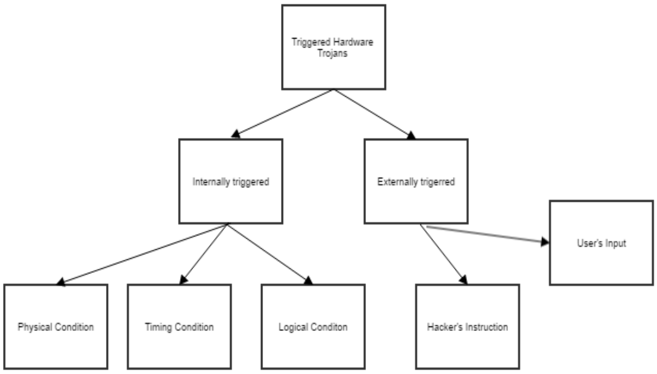

Figure 3: Classification of Triggered Hardware Trojans

## VIII INTERNALLY TRIGGERED

These Trojans start functioning when the chip attains some specific condition in terms of physical, logical or timing. They monitor the internal conditions of a chip and works accordingly.

***Physical Condition***: Trojans get triggered when parameters like temperature, pressure, stress, strain, etc., exceed a certain limit
***Logical Condition***: Trojans get triggered when circuits attain specific logical conditions that are predefined. They can be either combinational or sequential.
***Timing Condition***: These Trojans are embedded with a system clock and start working after a specified time.

## IX EXTERNALLY TRIGGERED

Designers and users can trigger these types of Trojans.

***User's Input***: These Trojans monitor the input signals from the user and get triggered when the user provides a specific input. This can happen without the user's knowledge.
***Hacker's Instruction***: Hackers monitor the network layer and identify weak spots. They can control the Network on Chip. Using this as an advantage they can externally trigger the Trojan using a specific instruction.

## X. TROJAN DETECTION TECHNIQUES

It is highly impossible to prevent Trojans due to the following reasons:

- Hardware Trojans are extremely small in size and difficult to identify in a large circuit
- They are stealthy in nature and this makes them almost impossible to detect.
- Use of third party IP cores during fabrication makes it impossible to verify them
- Software Trojans in CAD tools can introduce Hardware Trojans during design

Such complex conditions make Hardware Trojans almost impossible to prevent. Fortunately, there are few detection techniques that may help in avoiding serious consequences caused by Hardware Trojans.

Following are few detection techniques:

- Temperature Analysis

  When an extra circuit present in the IC generates extra heat, this can be compared with the real chip that functions normally. Temperature change can occur due to other reasons. Hence a detailed analysis is required.

- Power Based Analysis

  A Trojan when present in a circuit will consume different amount of current when compared to the normal one. Once this occurs, the Trojan can be detected, but its location cannot be found. This technique is challenging since change of power consumption will be very small and detecting this is difficult.

- Current Integration Technique

  In this technique, the flow of current is measured in each portion of the IC and if there is a presence of a Trojan in in the circuit, the flow changes at the that section. This measurement is again a sensitive task since Trojans need minimum amount of current and the detection & measurement of this current is very difficult and sensitive to perform. This process needs a golden model for detection.

All the described techniques are very tough and sensitive to carry out since the parameters they deal with are of miniscule magnitude. Also, a golden model of the entire System on Chip is required for each technique. These techniques do not provide any guarantee of presence of Trojan in a system. Currently there is no highly effective technique that can surely identify and locate a Hardware Trojan.

## XI. SIDE CHANNEL ATTACKS

In Side Channel Attacks, there is possibility of nodes revealing critical information, during normal operation [8]. An example of this attack will be the electromagnetic signature. Electro Magnetic waves that are emitted by the node, contain important information about the status and parameters of the device[1]. Hackers can use this as an advantage to retrieve data. Thus, privacy of data is at stake. Such attacks can prove to be dangerous in sectors like healthcare and military.

Few classes of side channel attacks include,

***Timing Attack***: Movement of data in and out of the CPU on the hardware performing cryptographic algorithms, is observed. Based on variations in time taken to process the cryptographic operations, the entire secret key can be obtained.
***Power Analysis Attack***: This type of attack observes the power consumption the hardware devices connected to the internet and can provide detailed information about the device.
***Cache Attack:*** The attacker monitors the cache access made by the victim in a shared physical system as in a cloud service or a in virtualized environment and attacks based on the pattern.

## XII. COUNTERMEASURES

- Filtering and Conditioning of power lines can help in block power-analysis attacks. This must be carried out cautiously since even very small correlations can compromise security.
- Jamming the emitted channel with noise can also help. As the amount of noise in the side channel increases, the attacker has to collect more measurements which becomes difficult for him.
- Displays in devices with special shielding can be used to lessen electromagnetic emissions, thus reducing data leakage.

## XIII. CONCLUSION

We have seen the different kind of attacks that the devices connected to IoT systems encounter. Many of them have few countermeasures that can keep them secure and working. Unfortunately, most of the them will not be able to handle attacks that are highly fierce since researchers have not yet come with highly concrete solutions that can help them tackle and stay secure. Both hardware and software departments have a lot of loopholes. To obtain an IoT enabled system that is 100% secure, one must fully secure both hardware and software levels without any compromise. While designing, one must plan for the worst and must leave no stone unturned, so that the system designed is well secured and possibilities of unauthorized access, especially with respect to data, are less. Both hardware and software threats depend on each other. Both Hardware Trojans and Side Channel Attacks are malicious but Trojans seem to be more troublesome. Securing devices from Hardware Trojans is definitely a challenge. Though there are measures (as we discussed) to prevent and tackle them, a highly effective mechanism to completely get rid of them has not yet been developed. Researchers are currently working on this critical issue. It is evident that IoT is going to be a very important part of life and hence, it is even more important to secure those related devices and systems effectively before we deploy them and use it in our everyday lives since privacy and security of huge amounts of data are at stake.

## XIV. REFERENCES

[1] Hardware Security Assurance in Emerging IoT Applications
Jaya Dofe, Jonathan Frey, and Qiaoyan Yu Department of Electrical and Computer Engineering
University of New Hampshire Durham, New Hampshire 03824, United States Email: qiaoyan.yu@unh.edu

[2] Proposed Embedded Security Framework for Internet of Things (IoT)
Sachin Babar1, Antonietta Stango1, Neeli Prasad1, Jaydip Sen2, Ramjee Prasad1
1Center for TeleInFrastruktur, Aalborg University , Aalborg , Denmark
2Tata Consultancy Services, Kolkata, India {sdb,as,np}@es.aau.dk, jaydip.sen@tcs.com, prasad@es.aau.dk

[3] The Internet of Things: An Overview, October 2015, The Internet Society

[4] 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, pghosal}@it.iiests.ac.in

[5] Cyber Security and the Internet of Things:Vulnerabilities, Threats, Intruders and Attacks
Mohamed Abomhara and Geir M. Køien Department of Information and Communication Technology, University of Agder, Norway Corresponding Authors: {Mohamed.abomhara; geir.koien}@uia.no Received 14 September 2014; Accepted 17 April 2015; Publication 22 May 2015

[6] Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures
Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan Department of Computer Science & Engineering American University of Sharjah, UAE- Presented In The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015)

[7] IoT Attacks-An Incident
http://www.businessinsider.com/internet-of-things-corporate-cyberattacks-2016-10

[8] A Comprehensive Study of Security of Internet-of-Things Arsalan Mohsen Nia, Student Member, IEEE and Niraj K. Jha, Fellow, IEEE