Executing an Effective IoT Security Testing Methodology: A Complete Guideline for Device Developers

BY

Amit Chakraborty Chhoton
ID: 163-25-537

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Science and Engineering

Supervised By

Dr. Syed Akhter Hossain
Professor
Department of CSE
DaffodilInternational University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

DECEMBER 2018

APPROVAL

This Project/internship titled **"Executing an Effective IoT Security Testing Methodology: A Complete Guideline for Device Developers"** submitted by Amit Chakraborty Chhoton, ID No: 163-25-537 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 28 November 2018.

BOARD OF EXAMINERS

____

Dr. Syed Akhter Hossain **Chairman**
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

____

Dr. Sheak Rashed Haider Noori **Internal Examiner**
Associate Professor& Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

____

Md. Zahid Hasan **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

____

Dr. Mohammad Shorif Uddin **External Examiner**
Professor
Department of Computer Science and Engineering
Jahangirnagar University

ABSTRACT

In IoT scenario, it's estimated that the amount of connected devices is predicted to grow exponentially to 50 billion by 2020. The deployment of sensors, actuators are increasing at a speedy pace around the world and IoT has gained intensive attention. A lot of smart services increase rapidly by the blessings of internet of things; however this coincides with a rise in security and privacy issues. Planning IoT testing strategy, it often times is it is well far through as it should be. Often here question like, we want to know that the IoT device is secure or how can we deploy application in a data scenario. But rarely does someone ask to prove that specific device is secure and it's a question that should be asked more often. HP security research did an evaluation and found that 70% IoT devices are vulnerable to an attack. Because IoT device are not tested properly and not follow a standard testing methodology. Therefore, we proposed a methodology based on testing approach that is able to effectively facilitate interactions of different stage of IoT device testing from technical point of view. These challenges are basically related to the IoT development pipeline, security, synchronization between on real-life environment and the adaptability imperatives of cutting edge IoT testing procedures.

TABLE OF CONTENTS

CONTENTS **PAGE**

CHAPTER

CHAPTER 5:- PROPOSED A TESTING METHODOLGY FOR THE INTERNET OF THINGS- A COMPLETE GUIDELINE FOR DEVELOPERS 40-49

CHAPTER 6:-DISCUSSION……………………………… 50-51

CHAPTER 7:- Conclusions…………………………………… 52

CHAPTER 8:-REFERENCES …………………………………. 53-56

LIST OF FIGURES

LIST OF TABLES

Chapter ONE

INTRODUCTION

1. Introduction

Internet of Things within their enterprises, production facilities are they ready right now to begin introducing smart products and products embedded intelligence. Some recent research was just completed with 350 manufactures across the United States and we think we are finding it really interesting. What we are going to talk about our executive summary of the results is titled the Internet of Things has finally arrived unfortunately aren’t ready because they are very much off mind about the testing process. Manufacturers are they ready for the Internet of Things? We have a lot about it there’s been a lot of hype we know there’s a lot of money being spent. One of the things that we wanted to take a look at about how manufacturers ready because of a disturbing finding we got in another study. In late 2017 a study of manufacturers in United States and what we found from that research 46 percent of manufacturing executives actually said they had no idea what the Internet of Things was. That’s why we decided to this piece of research to figure out well if we have got a lot of people who don’t know or not follow a standard methodology to testing Internet of Things. How can other manufacturers be ready for it? What we want to do though was do something little bit differently than most research out there. A lot of research looks at one side machine-to-machine communications, machine to enterprise.

1.1 Thesis Objective

The objective of this paper is to give an overview of how secure the Internet of Things and what security challenges have to be considered in arrange to convey a premise for a strong and secure IoT. This paper will help to understand the components the IoT is built of, the way they work, and which dangers each component faces. This approach leads to the taking after investigate following research questions:

- What are the security challenges of the IoT's key components ranging from secure boot, authentication, protected ports, secure storage, and secure connection?
- What are the currently known countermeasures for each component and how effective are they?
- Can the IoT as of today follow any testing methodology and already be considered secure?

1.2 Motivation

In late 2017 a study of manufacturers in United States and what we found from that research 46 percent of manufacturing executives actually said they had no idea what the Internet of Things was. That's why we decided to this piece of research to figure out well if we have got a lot of people who don't know or not follow a standard methodology to testing Internet of Things. How can other manufacturers be ready for it? What we want to do though was do something little bit differently than most research out there. A lot of research looks at one side machine-to-machine communications, machine to enterprise. The other side of the house they look at well smart products, intelligence products what's going on there. We wanted to look at how ready manufacturers are on both sides. We want to look in general are they ready for the Internet of Things, are they aware of it. How they are the taking the Internet of Things and Embedding it into their processes into their operations, into their production into their offices within their facilities and also take a look at are they ready right now to start developing, introducing and profiting from Internet of Things enabled products and what was found was really interesting.

1.3 Scope of the Thesis

The paper will focus exclusively on the IoT's security issue like secure boot, authentication, secured ports, secure storage and secure connection. All secure issue will be clarified in detail, counting data around their utilization inside the IoT as well as around their risks. The scope of this thesis incorporates all compelling countermeasures to overcome the current security issues, which can be depicted for each component. Besides, the countermeasures and their viability will be summarized and evaluated. The results and discoveries of this paper are based on the current literature available about the security issue of Internet of Things.

1.4 Predicting the Future

This is a big gap between the industries where a quality testing expert or QA person has fill the gap and has is having more opportunity the integration because both of them have a lab in each of the integration part. This is a biggest gap into industry where IoT and most importantly for a QA expert is having the biggest opportunity the integration part. We need to have the domain knowledge about the hardware part along with the domain knowledge. Don't need with coder into that we know how domain knowledge about both of them. So that when it comes to integration part when it comes to the gain data from cloud to the device from the data clouds. There were five machines and all those machines from same manufacturers were creating different type of data. So if we have don't have knowledge on the hardware part then the IT person who is actually analyzing the data and building the big data solutions won't be able to analyze that part because that IT person pretty much separated from the hardware part. Again integration has to be what people will try to do is like let's make device consume or have 10KB of RAM or let's say 20MB of RAM and lets use as we keep traditional stuff that we are using and let's make the system OK [12]. When it comes to developer eyes we have been also try to do is like we try to make it happen anyhow that's our main object us try to make things happen on the time. Again both the parties going to have limited alternative domain knowledge.**1.5**

Outline

There are four part of this thesis: background, challenges, solutions and guideline.

This background chapter will allow the crucial foundation material required to get it the specialized perspectives of this Proposition, as well as clarifying the establishment of the Internet of Things in common.

The challenges chapter will highlight the different challenges that exist in IoT today, as well as future challenges. There are some key differences from the challenges that exist in regular desktop computing, which stems from the constraints that exists in IoT that will affect the way security is handled in IoT devices.

The solutions chapter will present different solutions to the challenges presented in the challenges chapter. What and how challenges are implemented will be dictated by a proposed testing methodology.

Chapter Two

BACKGROUND

2.1 Introduction

In this section we want to describe some research that recently completed about the Internet of Things. More specifically that research was about how ready manufactures are or frankly aren't to implement the Internet of Things within their enterprises, production facilities are they ready right now to begin introducing smart products and products embedded intelligence. Some recent research was just completed with 350 manufactures across the United States and we think we are finding it really interesting. What we are going to talk about our executive summary of the results is titled the Internet of Things has finally arrived unfortunately aren't ready because they are very much off mind about the testing process. Manufacturers are they ready for the Internet of Things? We have a lot about it there's been a lot of hype we know there's a lot of money being spent. One of the things that we wanted to take a look at about how manufacturers ready because of a disturbing finding we got in another study. In late 2017 a study of manufacturers in United States and what we found from that research 46 percent of manufacturing executives actually said they had no idea what the Internet of Things was. That's why we decided to this piece of research to figure out well if we have got a lot of people who don't know or not follow a standard methodology to testing Internet of Things. How can other manufacturers be ready for it? What we want to do though was do something little bit differently than most research out there. A lot of research looks at one side machine-to-machine communications, machine to enterprise. The other side of the house they look at well smart products, intelligence products what's going on there. We wanted to look at how ready manufacturers are on both sides. We want to look in general are they ready for the Internet of Things, are they aware of it. How they are the taking the Internet of Things and Embedding it into their processes into their operations, into their production into their offices within their facilities and also take a look at are they ready right now to start developing, introducing and profiting from Internet of Things enabled products and what was found was really interesting.

2.2 Related Works

In recent years, many surveys were published to emphasize the advancement of research activities in the IoT framework [1], [2], [3], [4], [5], [6]. They mainly focus on general issues of IoT fundamentals or models. Security concerns were presented as a part of each survey and treated in a generic manner and security and privacy were often shown jointly as a single concept. Unfortunately, as illustrated in Table 1, none of the previous surveys has detailed in-depth security concerns of the IoT and figure 2.3 shows that last ten year attacks on IoT device.

TABLE 1. SURVEYS ON INTERNET OF THINGS SECURITY.

Survey	Citation	Year	IoT vision	Security issues
The Internet of Things: A survey	[2]	2010	Things-oriented, Internet-oriented and Semantic-oriented	Identification, authentication, integrity, privacy, trust
Internet of Things: A Vision, Architectural Elements,and Future Directions	[1]	2012	Cloud centric vision	Identification, authentication, integrity, privacy
Internet of things: Vision, applications and research challenges	[3]	2012	anything communicates, anything is identified, and anything interacts	Data confidentiality , privacy, trust
The Internet of Things: A Survey from the Data-Centric Perspective	[4]	2013	Things-oriented, Internet-oriented and Semantic-oriented	Identification, integrity, privacy
Towards Internet of Things: Survey and Future Vision	[5]	2013	3-Layer architecture, 5-Layer architecture	Physical security, privacy
Context Aware Computing for The Internet of Things: A Survey	[6]	2013	Things to be connected Anytime, Anyplace, with Anything and Anyone, using Any path, network and Any service.	Identification, privacy, trust

Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues	[7]	2015	5-Layer architecture	Authentication, integrity, confidentiality, trust, access control
Security, privacy and trust in Internet of Things: The road ahead	[8]	2015	A collection of smart devices that interact on a collaborative basis to fulfill a common goal	Privacy, trust, integrity, confidentiality, identification, authentication
Securing the Internet of Things Survey	[9]	2016	any-to-any connectivity	Authentication, access control, confidentiality
Internet of Things: A Review of Surveys Based on Context Aware Intelligent Services	[10]	2016	Different perspectives: services, connectivity, communication and networking viewpoints.	Privacy, integrity, access control, trust, identification.

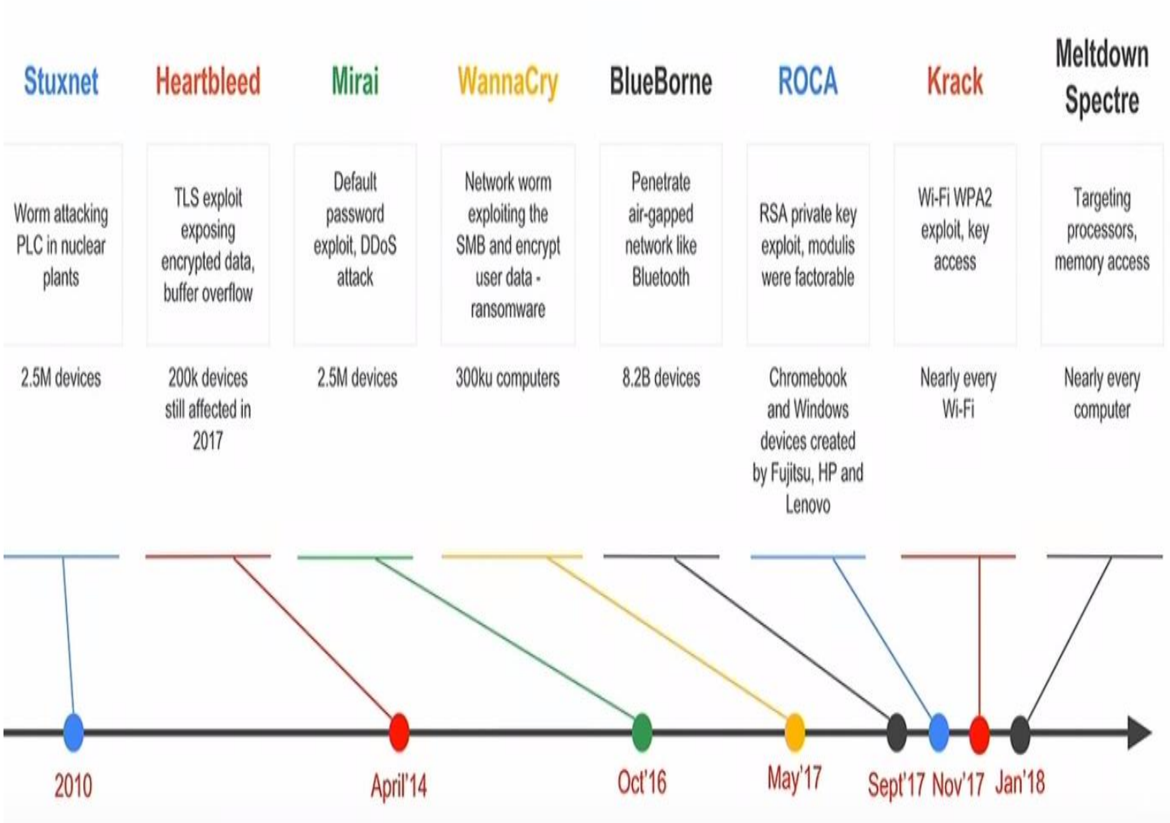
Stuxnet
Heartbleed
Mirai
WannaCry
BlueBorne
ROCA
Krack
Meltdown Spectre
Worm attacking PLC in nuclear plants
TLS exploit exposing encrypted data, buffer overflow
Default password exploit, DDoS attack
Network worm exploiting the SMB and encrypt user data - ransomware
Penetrate air-gapped network like Bluetooth
RSA private key exploit, modulis were factorable
Wi-Fi WPA2 exploit, key access
Targeting processors, memory access
2.5M devices
200k devices still affected in 2017
2.5M devices
300ku computers
8.2B devices
Chromebook and Windows devices created by Fujitsu, HP and Lenovo
Nearly every Wi-Fi
Nearly every computer
2010
April'14
Oct'16
May'17
Sept'17
Nov'17
Jan'18

Figure 2.3: Number of connected devices increases attention of hackers last ten years

2.3 Comparative Study

So we are going to get to that we want to talk about five things. We are going to talk about general awareness of the IoT, we are going to talk about are they using it within their processes are they using it within products, we are then going to talk about some deeper dive issues of particular interest around security etc and then we'll talk a little bit about who actually took the survey for us.So let's talk about IoT readiness within the facility and what's really interesting here when take a look at this data which as given as below.

Some manufacturers understand the potential of the IoT and figure 2.1 show the percentage of that fact.

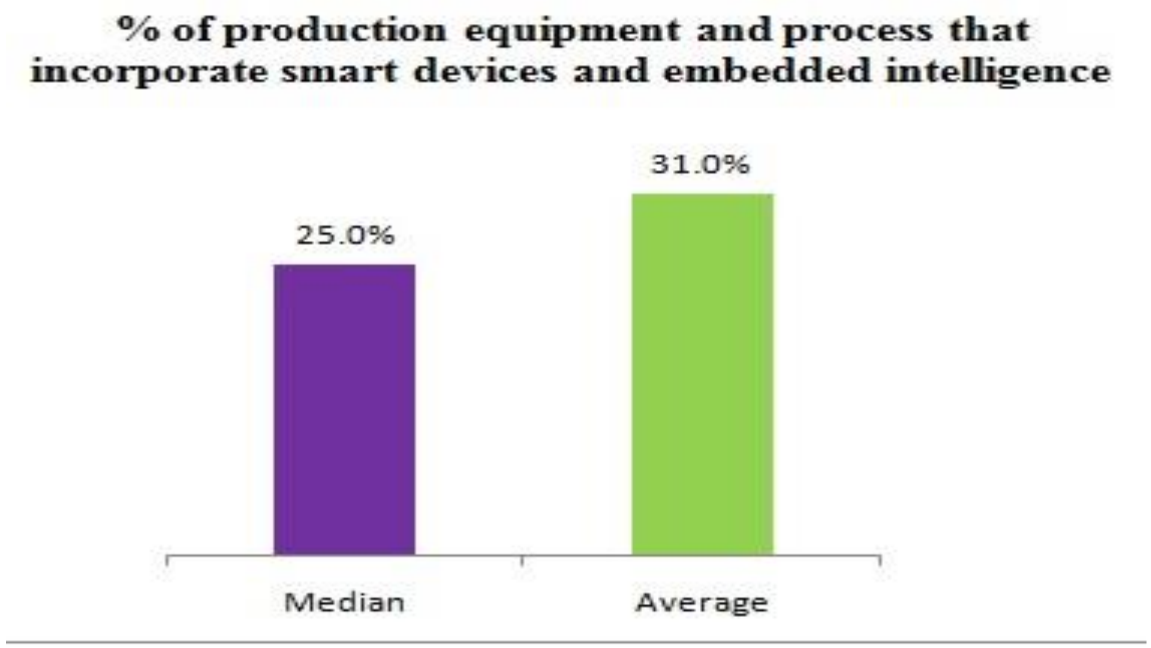

Figure 2.1: Potentiality of the IoT understand by manufacturers

Impact on their business:

- Only 17% report the IoT will have significant impact on their business.
- 36% report limited or no impact
- Impact on business in general:
- 24% report the IoT will have significant impact on their business.
- 29% report limited or no impact
-

When we take a look at have we implemented an IoT strategy the vast majority have not we have got only 12 percent who have follow IoT testing strategy. We have got a huge number you got 37 percent who say no: we don’t follow IoT testing strategy. Despite the fact that majority of manufacturers don’t have a plan or not follow any standard IoT testing methodology right now. They all expecting a lot more money on it over the next two years and they are all expecting magically to get profits out of within the next five years.

OT and IT collaboration is missing for many key IoT activities.

Two technology worlds have traditionally been soiled: operation technology (OT) departments and information technology departments.

Areas of OT/IT collaboration issues

- 53% resolve technical operation issues
- 50% network security
- 45% linking operations data with business analytics
- 45% upgrading legacy operation data with business analytics
- 45% upgrading legacy operating systems
- 45% upgrading legacy enterprise systems
- 37% upgrading technical enterprise issues

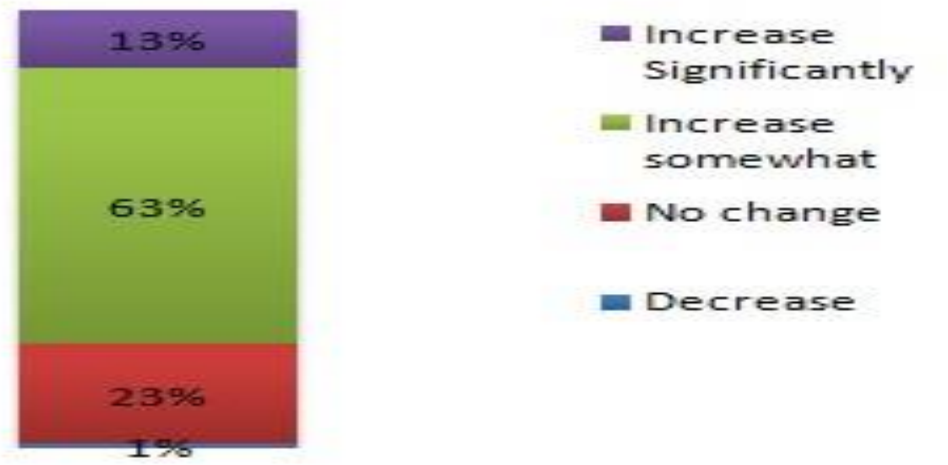

Figure 2.2: Some plant processes are managed via the IoT - with more to come.

Manufacturers must build out OT and OT/IT infrastructure
Network infrastructure accommodates IoT machine-to-machine communications (OT):

- 10% currently capable for machine-to-machine communications
- 41% some upgrades required
- 32% significant upgrades required
- 18% require network overhaul machine-to-machine communication

Network infrastructure accommodates IoT machine-to-enterprise communications (OT/IT):

- 13% currently capable for machine-to-enterprise communications
- 38% some upgrades required
- 35% significant upgrades required
- 18% require network overhaul machine-to-enterprise communication

2.4 Scope of the Problem

In this section we want to describe some research that recently completed about the Internet of Things and scope of the problem. More specifically that research was about how ready manufactures are or frankly are not to implement the Internet of Things within their enterprises, production facilities are they ready right now to begin introducing smart products and products embedded intelligence. Some recent research was just completed with 350 manufactures across the United States and we think we are finding it really interesting. What we are going to talk about our executive summary of the results is titled the Internet of Things has finally arrived unfortunately are not ready because they are very much off mind about the testing process. Manufacturers are they ready for the Internet of Things? In late 2017 a study of manufacturers in United States and what we found from that research 46 percent of manufacturing executives actually said they had no idea what the Internet of Things was. The fourth industrial revolution (Industry 4.0) enables the integration of information technology with industrial technology. The adoption of Industry 4.0 includes many complex technologies that come with challenges for many organizations [11]. That’s why we decided to this piece of research to figure out well if we have got a lot of people who don’t know or not follow a standard methodology to testing Internet of Things. So challenge in testing includes when it comes to most importantly IoT testing. So before building the system we should check with that operating systems and all the stuff we are using proper secure using. So just don't find them prevent them so that works do not comes into the picture or we have certain silent mode which everything will be updated from the provider and we won't need to put much of you into security stuff. Another point is what right now we have sort of people let's say that IoT is kind of combination of hardware plus cloud. Now when it comes to the professionals or experts so people who are into IT they are much more stick that I know cloud , I know networking, I know application development, I now the web development but I don't know about the hardware part. People worry who are into hardware they are very much separated from the IT part. This is a big gap between the industries where a quality testing expert or QA person has fill the gap and has is having more opportunity the integration because both of them have a lab in each of the integration part. This is a biggest gap into industry where IoT and most importantly for a QA expert is having the biggest opportunity the integration part. We need to have the domain knowledge about the hardware part along with the domain knowledge. Don't need with coder into that we know how domain knowledge about both of them. So that when it comes to integration part when it comes to the gain data from cloud to the device from the data clouds. There were five machines and all those machines from same manufacturers were creating different type of data. So if we have don't have knowledge on the hardware part then the IT person who is actually analyzing the data and building the big data solutions won't be able to analyze that part because that IT person pretty much separated from the hardware part. Again integration has to be what people will try to do is like let's make device consume or have 10KB of RAM or let's say 20MB of RAM and lets use as we keep traditional stuff that we are using and let's make the system OK [12]. When it comes to developer eyes we have been also try to do is like we try to make it happen anyhow that's our main object us try to make things happen on the time. Again both the parties going to have limited alternative domain knowledge. So here the role of a QA expert comes up. Again testers with domain knowledge multi-user application distributed environment deployment this is very important part. When it comes to deployment part the traditional stuff which we used to deploy like our website is run in a browser nothing more or we can have browsers in our smart phone, we just need to make them part a little smart phone size and this size particular stuff. When it comes to IoT related application IoT is being deployed in distributed environments. Some hardware part we have, some integration networking part we have, some cloud parts, some front-end part we have. Probably the product if we are into consumer IoT product part that we are developing might work very well in our own country, might not work very well in a certain other country or certain part of our own country.

2.5 Challenges

So challenge in testing includes when it comes to most importantly IoT testing. So before building the system we should check with that operating systems and all the stuff we are using proper secure using. So just don’t find them prevent them so that works do not comes into the picture or we have certain silent mode which everything will be updated from the provider and we won’t need to put much of you into security stuff. Another point is what right now we have sort of people let's say that IoT is kind of combination of hardware plus cloud. Now when it comes to the professionals or experts so people who are into IT they are much more stick that I know cloud , I know networking, I know application development, I now the web development but I don’t know about the hardware part. People worry who are into hardware they are very much separated from the IT part. This is a big gap between the industry where a quality testing expert or QA person has fill the gap and has is having more opportunity the integration because both of them have a lab in each of the integration part. This is a biggest gap into industry where IoT and most importantly for a QA expert is having the biggest opportunity the integration part. We need to have the domain knowledge about the hardware part along with the domain knowledge. Don’t need with coder into that we know how domain knowledge about both of them. So that when it comes to integration part when it comes to the gain data from cloud to the device from the data clouds. There were five machines and all those machines from same manufacturers were creating different type of data. So if we have don’t have knowledge on the hardware part then the IT person who is actually analyzing the data and building the big data solutions won't be able to analyze that part because that IT person pretty much separated from the hardware part. Again integration has to be what people will try to do is like let’s make device consume or have 10KB of RAM or let’s say 20MB of RAM and let’s use as we keep traditional stuff that we are using and let’s make the system ok. When it comes to developer eyes we have been also try to do is like we try to make it happen anyhow that’s our main object us try to make things happen on the time. Again both the parties going to have limited alternative domain knowledge. So here the role of a QA expert comes up. Again testers with domain knowledge multi-user application distributed environment deployment this is very important part. When it comes to deployment part the traditional stuff which we used to deploy like our website is run in a browser nothing more or we can have browsers in our smart phone, we just need to make them part a little smart phone size and this size particular stuff. When it comes to IoT related application IoT is being deployed in distributed environments. Some hardware part we have, some integration networking part we have, some cloud parts, some front-end part we have. Probably the product if we are into consumer IoT product part that we are developing might work very well in our own country, might not work very well in a certain other country or certain part of our own country.

Chapter Three

Security Challenges in the Internet of Things

3.1 Authorization

More specifically that research was about how ready manufactures are or frankly are not to implement the Internet of Things within their enterprises, production facilities are they ready right now to begin introducing smart products and products embedded intelligence. Some recent research was just completed with 350 manufactures across the United States and we think we are finding it really interesting. What we are going to talk about our executive summary of the results is titled the Internet of Things has finally arrived unfortunately are not ready because they are very much off mind about the testing process. Manufacturers are they ready for the Internet of Things? In late 2017 a study of manufacturers in United States and what we found from that research 46 percent of manufacturing executives actually said they had no idea what the Internet of Things was. The fourth industrial revolution (Industry 4.0) enables the integration of information technology with industrial technology. The adoption of Industry 4.0 includes many complex technologies that come with challenges for many organizations [11]. That's why we decided to this piece of research to figure out well if we have got a lot of people who don't know or not follow a standard methodology to testing Internet of Things. So challenge in testing includes when it comes to most importantly IoT testing. So before building the system we should check with that operating systems and all the stuff we are using proper secure using. Table 2: Table of challenges, what the result of the challenge is, what constraints they are related to, and the possible solutions.

Challenges	Results	Related Constraints	Solution
Authentication	False data can be treated as correct	Processing, Bandwidth, Power	Authenticated encryption
Authorization	Adversary access to important data and functions	Processing, bandwidth, Power	Authorization
Availability	Delayed updates, management	Power, Bandwidth	Work with existing Restrictions
Lacking multi-layer security	No added security if one fails	Processing, Bandwidth, Power	Use encryption on multiple levels
Key distribution	Key can be snapped up during transit	Processing, Bandwidth, Power	Use case specific. Different solutions.
Prost production Management	Backdoors can be introduced to the system	Bandwidth	Authorization, Authentication, Network Encryption
Privacy	Ability to track users		Privacy
DoS	Render device unusable, loss of data	Processing, Bandwidth, Power	Detection, Network Design
Unintended uses	Ability to track users		Always prioritize security
Usability Before security	No added security if one fails		User friendly security. Always include security.
Local Storage	False data can be treated as correct	Bandwidth	Use case specific. Offloading possible?
Local Processing	Adversary access to important data and functions	Power, Processing	Increased processing. Offloading possible?
Interoperability	No devices talks with each other, extra layer needed (added breakpoint)	Processing, Bandwidth	Adaption, corporate Unity

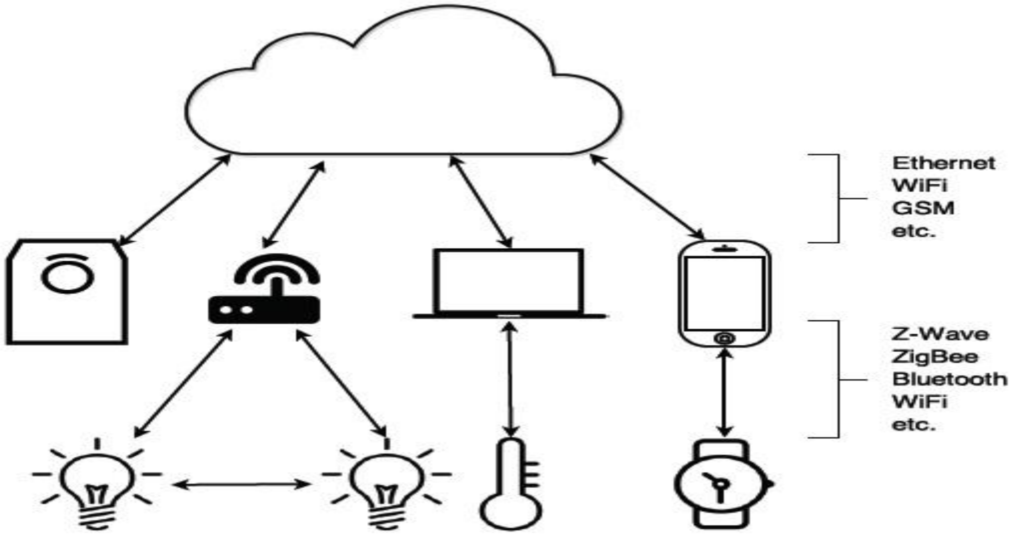

Figure 3.1: Scenario of authorization

3.2.2 Authentication

Any time you connect an embedded device to a network it's going to be subjected to a wide variety of security risks. IOT all about connectivity, so we know our devices are going to be connected. Some of the security risks that we'll be talking about in this paper are eavesdropping attacks, man-in-the-middle attacks, unauthorized access and control product cloning and unauthorized overproduction. Really anything you can do across the network to access or disrupt a device. As you know embedded controllers can be entry points for cyber attacks. The German steel mill that was attacked was as a result hackers coming in through the corporate network and then able to move unilaterally throughout the control network or the operational network without any defences in place. The target data breach once hackers were inside the network they were able to communicate with the embedded devices with impunity. In order to control the access to our devices, we need to ensure that we've got both secure communication and authentication. Securing communication is really a matter of adding the right protocols to control and encrypt a communication with our device. Tos and its cousin D TLS or data link TLS are commonly used protocols and embedded devices. Depending on your use case other protocols may be appropriate SSH,IpSec and Ike are often used in IP networks and many of the wireless standards have their own communication security protocols. In terms of authentication for embedded devices there are really two types of authentication. The fast is user authentication and it's a human being who's trying to access the device authorized to do so. The traditional method is simply to use a password management system. The key here is to actually implement strong passwords. Every year there's a number of new data breaches and in which passwords are discovered and if you do the research and go read them it's always the same passwords that are used over and over again they never change. People are inclined to use easiest password. If you allow your users to do this then your devices will be easily breached with simple dictionary attacks. Depending on the device you're building and the nature of its use other types of authentication might make sense. Biometric authentication could be used or a second factor authentication mechanism. The other type of identification mechanism is machine to machine authentication. So how do you know that your device is talking to another machine that's really authorized to perform the action? Oftentimes this is done using certificates and public key infrastructure. When looking at the PKI infrastructure we want to adopt we also have to decide what we're going to use a public or a private certificate authority. Certificate management for the IOT, again we can use the public certificate authority. This is what our web browser uses when I go to amazon.com to make a purchase. Our web browser verifies that the website amazon.com is really who it says it is by validating its certificate and it's reliant on a public certificate. Authority as part of that process so this enables what we call worldwide trust and requires external integration with a public certificate authority. This model may be appropriate for an IOT device. The other approach is use to a private certificate authority. Essentially having a certificate authority that works in a closed world, so that all the devices that are enrolled with that certificate authority can validate each other using certificates but without reliance on any external third-party. The other factor is that when we go to amazon.com doesn't use a certificate to validate us. It requires meet the enter our username and password to verify that we are who say we are. In the embedded world when we do machine to machine authentication each device has a certificate so we can do is called mutual authentication. So each device validates the other. Obviously a machine to machine authentication we don't have a user entering a password or providing biometric authentication so two-way authentication is performed using certificates. The other thing needed then is device side support. So the certificate authority provides the management structure on the PKI for distributing certificates, validating certificates and managing certificates. But device itself must have the ability to securely store validate and use certificates and must support things such as SCP e or other certificate authority protocols in this process.

3.2.3 Availability

The services conveyed by IoT systems must always be accessible to approved substances. Availability is a fundamental feature of a fruitful sending of IoT systems. However, IoT frameworks and devices can still be rendered unavailable by numerous dangers, such as DoS or dynamic jamming. Therefore, guaranteeing the persistent availability of IoT services to users may be a basic property of IoT security.

3.2.4 Confidentiality

Confidentiality could be a crucial security characteristic of IoT systems. IoT devices may store and exchange delicate data that should not be uncovered by unauthorized people. Medical (understanding related), individual, the IoT system is challenging. To fulfill the required security prerequisite, the arrangement ought to incorporate all encompassing considerations. In any case, IoT gadgets for the most part work in an unattended environment. Subsequently, an intruder may physically get to these devices. IoT gadgets are ordinarily associated over remote systems where an intruder might uncover private data from the communication channel by eavesdropping. IoT devices cannot back complex security structures since of their limited computation and control assets [13]. Hence, securing the IoT system may be a complex and challenging assignment. Given that the most objective of the IoT framework is to be accessed by anybody, anyplace and anytime, assault vectors or surfaces also become open to attackers [14, 15]. Thus, causing potential threats to ended up more likely. A threat is an act that can misuse security shortcomings in a system and applies a negative effect on it [13]. Various threats, such as detached assaults (e.g. listening in) and dynamic dangers (e.g. spoofing, Sybil, man-in-the-middle, malevolent inputs and dissent of benefit (DoS)), might influence the IoT framework. Figure 4 appears the potential assaults that can influence the most security necessities (verification, integrity no repudiation, privacy accessibility and authorization).

3.2.5 Key Distribution

IOT all about connectivity, so we know our devices are going to be connected. Some of the security risks that we'll be talking about in this paper are eavesdropping attacks, man-in-the-middle attacks, unauthorized access and control product cloning and unauthorized overproduction. Really anything you can do across the network to access or disrupt a device. As you know embedded controllers can be entry points for cyber attacks. The German steel mill that was attacked was as a result hackers coming in through the corporate network and then able to move unilaterally throughout the control network or the operational network without any defences in place. The target data breach once hackers were inside the network they were able to communicate with the embedded devices with impunity. In order to control the access to our devices, we need to ensure that we've got both secure communication and authentication. Securing communication is really a matter of adding the right protocols to control and encrypt a communication with our device. [16] [17].

3.2.6 Post-Production Management

The German steel mill that was attacked was as a result hackers coming in through the corporate network and then able to move unilaterally throughout the control network or the operational network without any defences in place. The target data breach once hackers were inside the network they were able to communicate with the embedded devices with impunity. In order to control the access to our devices, we need to ensure that we've got both secure communication and authentication. Securing communication is really a matter of adding the right protocols to control and encrypt a communication with our device. Tos and its cousin D TLS or data link TLS are commonly used protocols and embedded devices. Depending on your use case other protocols may be appropriate SSH,IpSec and Ike are often used in IP networks and many of the wireless standards have their own communication security protocols. In terms of authentication for embedded devices there are really two types of authentication. The fast is user authentication and it's a human being who's trying to access the device authorized to do so. The traditional method is simply to use a password management system. The key here is to actually implement strong passwords. Every year there’s a number of new data breaches and in which passwords are discovered and if you do the research and go read them it’s always the same passwords that are used over and over again they never change.

3.2.7 Privacy

Some of the security risks that we’ll be talking about in this paper are eavesdropping attacks, man-in-the-middle attacks, unauthorized access and control product cloning and unauthorized overproduction. Really anything you can do across the network to access or disrupt a device. As you know embedded controllers can be entry points for cyber attacks. The German steel mill that was attacked was as a result hackers coming in through the corporate network and then able to move unilaterally throughout the control network or the operational network without any defences in place. The target data breach once hackers were inside the network they were able to communicate with the embedded devices with impunity. In order to control the access to our devices, we need to ensure that we’ve got both secure communication and authentication. Securing communication is really a matter of adding the right protocols to control and encrypt a communication with our device. [21]. Figure 3.2 shows that the heat map of power uses versus time.

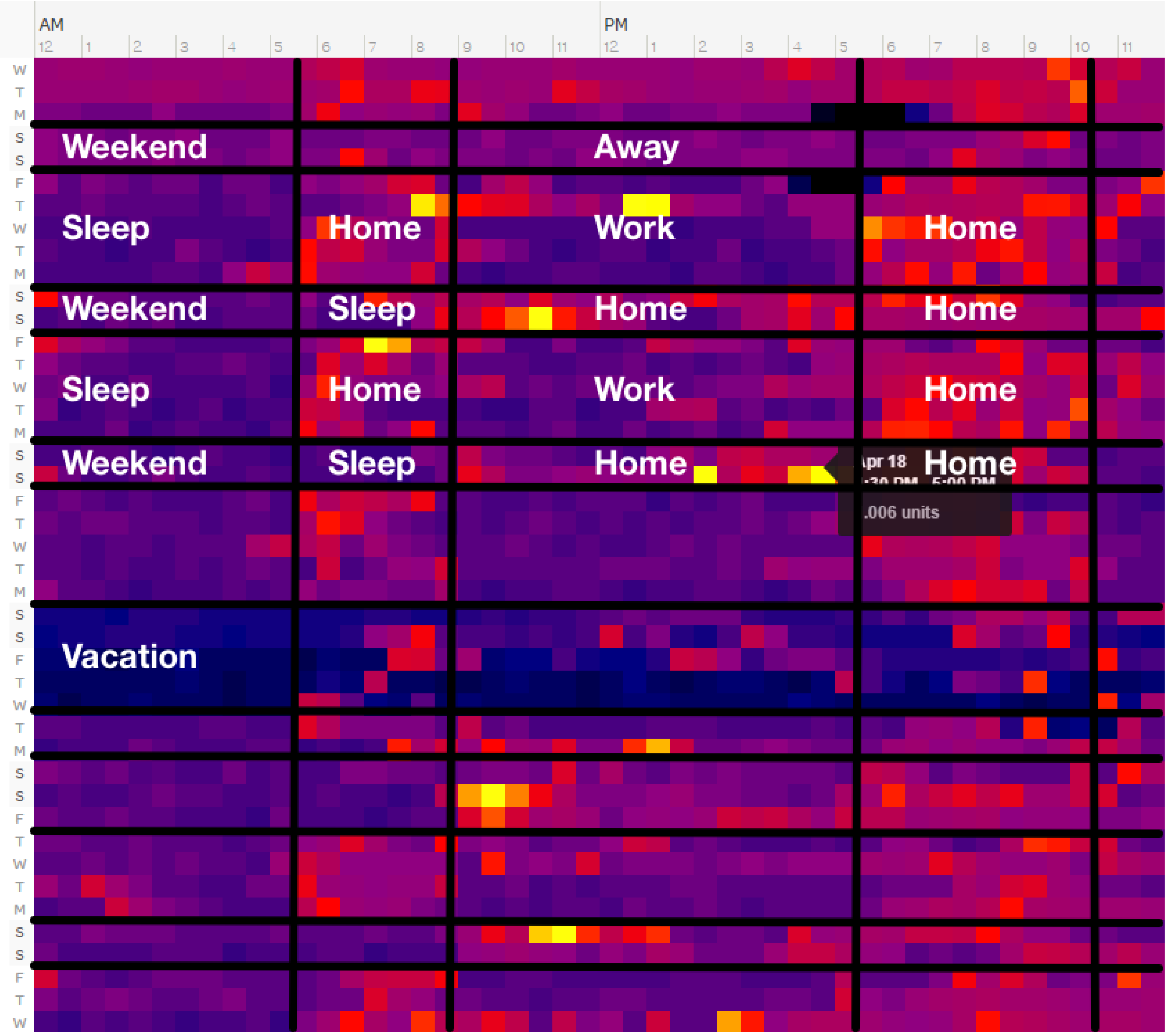

Figure 3.2: Heat map of power usage versus time. The power company can deduce a lot about its users by using simple analysis. Original heat map without analysis by: Powershop Australia Pty Ltd.

3.2.8 Denial of Service

IOT all about connectivity, so we know our devices are going to be connected. Some of the security risks that we'll be talking about in this paper are eavesdropping attacks, man-in-the-middle attacks, unauthorized access and control product cloning and unauthorized overproduction. Really anything you can do across the network to access or disrupt a device. As you know embedded controllers can be entry points for cyber attacks. The German steel mill that was attacked was as a result hackers coming in through the corporate network and then able to move unilaterally throughout the control network or the operational network without any defences in place. The target data breach once hackers were inside the network they were able to communicate with the embedded devices with impunity. In order to control the access to our devices, we need to ensure that we’ve got both secure communication and authentication. Securing communication is really a matter of adding the right protocols to control and encrypt a communication with our device. Tos and its cousin D TLS or data link TLS are commonly used protocols and embedded devices. Depending on your use case other protocols may be appropriate SSH,IpSec and Ike are often used in IP networks and many of the wireless standards have their own communication security protocols. In terms of authentication for embedded devices there are really two types of authentication. The fast is user authentication and it’s a human being who’s trying to access the device authorized to do so. The traditional method is simply to use a password management system. The key here is to actually implement strong passwords. Every year there’s a number of new data breaches and in which passwords are discovered and if you do the research and go read them it’s always the same passwords that are used over and over again they never change. People are inclined to use easiest password. If you allow your users to do this then your devices will be easily breached with simple dictionary attacks. Depending on the device you’re building and the nature of its use other types of authentication might make sense.

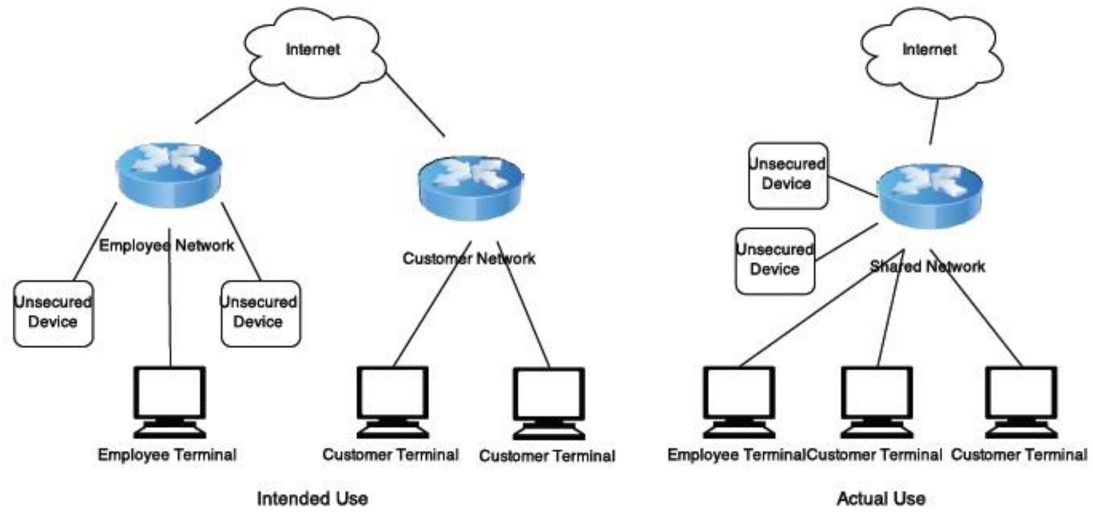

Figure 3.3: Illustrating the Sonos case of an unintended use-case where the developers assumed the device would be used on a secure network

3.2.9 Unintended uses

We'll be talking about in this paper are eavesdropping attacks, man-in-the-middle attacks, unauthorized access and control product cloning and unauthorized overproduction. Really anything you can do across the network to access or disrupt a device. As you know embedded controllers can be entry points for cyber attacks. The German steel mill that was attacked was as a result hackers coming in through the corporate network and then able to move unilaterally throughout the control network or the operational network without any defences in place. The target data breach once hackers were inside the network they were able to communicate with the embedded devices with impunity. In order to control the access to our devices, we need to ensure that we've got both secure communication and authentication. Securing communication is really a matter of adding the right protocols to control and encrypt a communication with our device. [23].

3.2.10 Usability before Security

In order to control the access to our devices, we need to ensure that we’ve got both secure communication and authentication. Securing communication is really a matter of adding the right protocols to control and encrypt a communication with our device. Tos and its cousin D TLS or data link TLS are commonly used protocols and embedded devices. Depending on your use case other protocols may be appropriate SSH,IpSec and Ike are often used in IP networks and many of the wireless standards have their own communication security protocols. In terms of authentication for embedded devices there are really two types of authentication. The fast is user authentication and it’s a human being who’s trying to access the device authorized to do so. The traditional method is simply to use a password management system. The key here is to actually implement strong passwords. Every year there’s a number of new data breaches and in which passwords are discovered and if you do the research and go read them it’s always the same passwords that are used over and over again they never change. People are inclined to use easiest password. If you allow your users to do this then your devices will be easily breached with simple dictionary attacks.

Chapter Four

Solution to challenges in the internet of things

This chapter will present current and future solutions to the challenges within IoT, and current and future recommendations for securing IoT systems. As the solutions are dependent on the available resources, some topics will include different solutions based on the constraints.

4.1 Authorization

We know that Internet of Things is a huge story about everything that surrounds us we can digitize and connect to the internet. In figure 5.2 shows the complete IoT product ecosystem. So the ecosystem of the Inter- net of Things consists of various kinds of devices. It can be cars with artificial intelligence, smart industry, smart city, infrastructure or it can be wearable electronics or some sensors. Assets in any IoT ecosystem can be hardware, computer program, or a chunk of information (having a place to people or participate organizations), administrations, or the data in that [40]. Main requirement of IoT product ecosystem have to be identified and integrated into communication network.

4.2 Authentication

Any time you connect an embedded device to a network it's going to be subjected to a wide variety of security risks. IOT all about connectivity, so we know our devices are going to be connected. Some of the security risks that we'll be talking about in this paper are eavesdropping attacks, man-in-the-middle attacks, unauthorized access and control product cloning and unauthorized overproduction. Really anything you can do across the network to access or disrupt a device. As you know embedded controllers can be entry points for cyber attacks. The German steel mill that was attacked was as a result hackers coming in through the corporate network and then able to move unilaterally throughout the control network or the operational network without any defences in place. The target data breach once hackers were inside the network they were able to communicate with the embedded devices with impunity. In order to control the access to our devices, we need to ensure that we've got both secure communication and authentication. Securing communication is really a matter of adding the right protocols to control and encrypt a communication with our device. Tos and its cousin D TLS or data link TLS are commonly used protocols and embedded devices. Depending on your use case other protocols may be appropriate SSH,IpSec and Ike are often used in IP networks and many of the wireless standards have their own communication security protocols. In terms of authentication for embedded devices there are really two types of authentication. The fast is user authentication and it's a human being who's trying to access the device authorized to do so. The traditional method is simply to use a password management system. The key here is to actually implement strong passwords. Every year there's a number of new data breaches and in which passwords are discovered and if you do the research and go read them it's always the same passwords that are used over and over again they never change. People are inclined to use easiest password. [27].

4.3.2 Optimized Protocols

IOT all about connectivity, so we know our devices are going to be connected. Some of the security risks that we'll be talking about in this paper are eavesdropping attacks, man-in-the-middle attacks, unauthorized access and control product cloning and unauthorized overproduction. Really anything you can do across the network to access or disrupt a device. As you know embedded controllers can be entry points for cyber attacks. The German steel mill that was attacked was as a result hackers coming in through the corporate network and then able to move unilaterally throughout the control network or the operational network without any defences in place. The target data breach once hackers were inside the network they were able to communicate with the embedded devices with impunity. In order to control the access to our devices, we need to ensure that we've got both secure communication and authentication. Securing communication is really a matter of adding the right protocols to control and encrypt a communication with our device. Tos and its cousin D TLS or data link TLS are commonly used protocols and embedded devices. Depending on your use case other protocols may be appropriate SSH,IpSec and Ike are often used in IP networks and many of the wireless standards have their own communication security protocols. In terms of authentication for embedded devices there are really two types of authentication. The fast is user authentication and it's a human being who's trying to access the device authorized to do so. The traditional method is simply to use a password management system. The key here is to actually implement strong passwords. Every year there's a number of new data breaches and in which passwords are discovered and if you do the research and go read them it's always the same passwords that are used over and over again they never change. People are inclined to use easiest password. If you allow your users to do this then your devices will be easily breached with simple dictionary attacks. Depending on the device you're building and the nature of its use other types of authentication might make sense. [19].

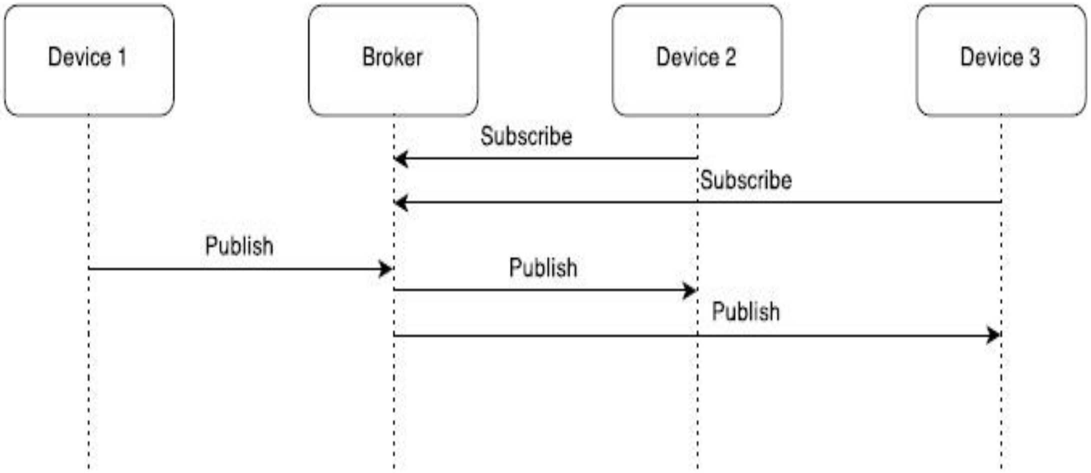

Figure 4.1: Illustration of the publisher / subscriber method used by MQTT to reduce bandwidth overhead

4.4 Application Layer Encryption

Any time you connect an embedded device to a network it’s going to be subjected to a wide variety of security risks. IOT all about connectivity, so we know our devices are going to be connected. Some of the security risks that we’ll be talking about in this paper are eavesdropping attacks, man-in-the-middle attacks, unauthorized access and control product cloning and unauthorized overproduction. Really anything you can do across the network to access or disrupt a device. As you know embedded controllers can be entry points for cyber attacks. The German steel mill that was attacked was as a result hackers coming in through the corporate network and then able to move unilaterally throughout the control network or the operational network without any defences in place. The target data breach once hackers were inside the network they were able to communicate with the embedded devices with impunity. In order to control the access to our devices, we need to ensure that we’ve got both secure communication and authentication. Securing communication is really a matter of adding the right protocols to control and encrypt a communication with our device. Tos and its cousin D TLS or data link TLS are commonly used protocols and embedded devices. Depending on your use case other protocols may be appropriate SSH,IpSec and Ike are often used in IP networks and many of the wireless standards have their own communication security protocols. In terms of authentication for embedded devices there are really two types of authentication. The fast is user authentication and it’s a human being who’s trying to access the device authorized to do so. The traditional method is simply to use a password management system. The key here is to actually implement strong passwords. Every year there’s a number of new data breaches and in which passwords are discovered and if you do the research and go read them it’s always the same passwords that are used over and over again they never change. People are inclined to use easiest password.

4.5 Public Key Infrastructure

IOT all about connectivity, so we know our devices are going to be connected. Some of the security risks that we’ll be talking about in this paper are eavesdropping attacks, man-in-the-middle attacks, unauthorized access and control product cloning and unauthorized overproduction. Really anything you can do across the network to access or disrupt a device. As you know embedded controllers can be entry points for cyber attacks. The German steel mill that was attacked was as a result hackers coming in through the corporate network and then able to move unilaterally throughout the control network or the operational network without any defences in place. The target data breach once hackers were inside the network they were able to communicate with the embedded devices with impunity. In order to control the access to our devices, we need to ensure that we’ve got both secure communication and authentication. Securing communication is really a matter of adding the right protocols to control and encrypt a communication with our device. Tos and its cousin D TLS or data link TLS are commonly used protocols and embedded devices. Depending on your use case other protocols may be appropriate SSH,IpSec and Ike are often used in IP networks and many of the wireless standards have their own communication security protocols. In terms of authentication for embedded devices there are really two types of authentication. The fast is user authentication and it’s a human being who’s trying to access the device authorized to do so. The traditional method is simply to use a password management system. The key here is to actually implement strong passwords. Every year there’s a number of new data breaches and in which passwords are discovered and if you do the research and go read them it’s always the same passwords that are used over and over again they never change. People are inclined to use easiest password. If you allow your users to do this then your devices will be easily breached with simple dictionary attacks. Depending on the device you’re building and the nature of its use other types of authentication might make sense.

4.7 Privacy

Paste Article Duplication Processing Re-Write Suggestion Done (unique Article) Privacy may be a troublesome topic at intervals IoT. On one hand, we would like to be able to acknowledge all devices unambiguously, however at a similar time; the user of the device usually doesn't would like to be recognized. Wireless networks like Wi-Fi or Bluetooth use distinctive identifiers (addresses) for every network interface that is broadcast in each transmission to or from the device. These distinctive identifiers was shown within the analysis of the EyeFi card, wherever the network interface broadcasts a Mack address with every packet, within the Fitbit wherever the device address was distinctive may track a person’s movement, and within the Home simple system wherever the ID of the transmitter is broadcasted with every signal. Once one needs to send information specifically to at least one receiver, this symbol is employed as associate degree address for the receiver to be able to establish the sender and contrariwise. In broadcasts directed at anyone United Nations agency needs to pay attention, however, these addresses don't seem to be extremely required and excluding or randomizing these will give privacy for the user. This feature is already incorporated into the Bluetooth LE normal once broadcasting advertisement frames (although not usually implemented), and square measure utilized by some vendors for Wi-Fi probes (e.g. Apple’s iPhone). Wherever this feature doesn't disallow the utilization of the merchandise, it ought to be enforced. However in several circumstances, the individuality of the device ID is that the whole purpose of the device. Associate degree example of this is often Bluetooth “bag/key/remote-trackers”. The likelihood of randomizing the address to avoid privacy issues isn't a break, as unambiguously chase the device is that the marketing feature of a Bluetooth tracker.

4.9 Data Storage

Any time you connect an embedded device to a network it’s going to be subjected to a wide variety of security risks. IOT all about connectivity, so we know our devices are going to be connected. Some of the security risks that we’ll be talking about in this paper are eavesdropping attacks, man-in-the-middle attacks, unauthorized access and control product cloning and unauthorized overproduction. Really anything you can do across the network to access or disrupt a device. As you know embedded controllers can be entry points for cyber attacks. The German steel mill that was attacked was as a result hackers coming in through the corporate network and then able to move unilaterally throughout the control network or the operational network without any defences in place. The target data breach once hackers were inside the network they were able to communicate with the embedded devices with impunity. In order to control the access to our devices, we need to ensure that we’ve got both secure communication and authentication. Securing communication is really a matter of adding the right protocols to control and encrypt a communication with our device. Tos and its cousin D TLS or data link TLS are commonly used protocols and embedded devices. Depending on your use case other protocols may be appropriate SSH,IpSec and Ike are often used in IP networks and many of the wireless standards have their own communication security protocols. In terms of authentication for embedded devices there are really two types of authentication. The fast is user authentication and it’s a human being who’s trying to access the device authorized to do so. The traditional method is simply to use a password management system. The key here is to actually implement strong passwords. Every year there’s a number of new data breaches and in which passwords are discovered and if you do the research and go read them it’s always the same passwords that are used over and over again they never change. People are inclined to use easiest password.

Chapter Five

Proposed a testing methodology for the Internet of Things - a Guideline for Developers

In this paper we proposed a methodology for testing IoT device based on our background study. In our proposed methodology figure 5.1 we are showing a flow chart about IoT testing methodology for testing IoT device which is as given as below:

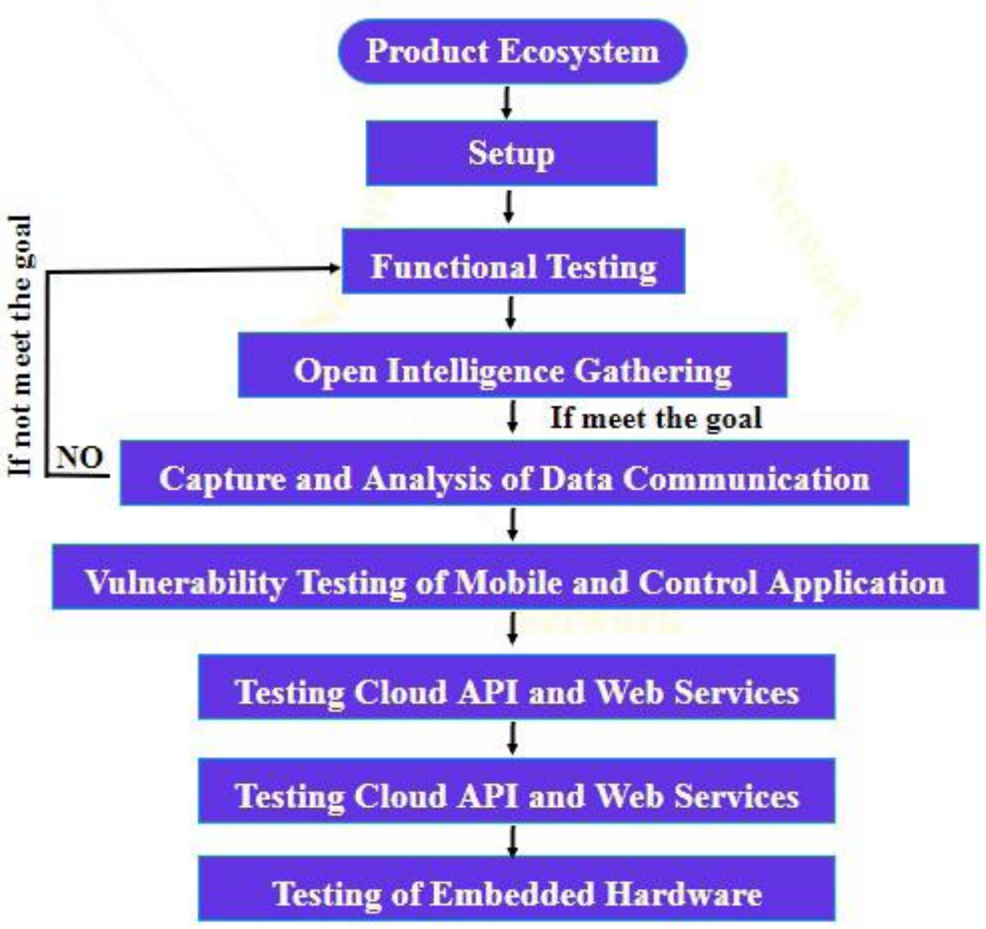
Product Ecosystem
Setup
Functional Testing
Open Intelligence Gathering
If meet the goal
If not meet the goal
NO
Capture and Analysis of Data Communication
Vulnerability Testing of Mobile and Control Application
Testing Cloud API and Web Services
Testing Cloud API and Web Services
Testing of Embedded Hardware

Figure 5.1. Proposed IoT Testing Methodology.

5.1 Product Ecosystem

We know that Internet of Things is a huge story about everything that surrounds us we can digitize and connect to the internet. In figure 5.2 shows the complete IoT product ecosystem. So the ecosystem of the Inter- net of Things consists of various kinds of devices. It can be cars with artificial intelligence, smart industry, smart city, infrastructure or it can be wearable electronics or some sensors. Assets in any IoT ecosystem can be hardware, computer program, or a chunk of information (having a place to people or participate organizations), administrations, or the data in that [40]. Main requirement of IoT product ecosystem have to be identified and integrated into communication network. Here under communication network we usually understand wireless networks wireless standards such as Wi-Fi, Bluetooth RFID, NFC Zigbee Laura bong it can be even narrow band LTE or future 5G networks with base station, hubs controller and other infrastructure to collect million numbers of devices to

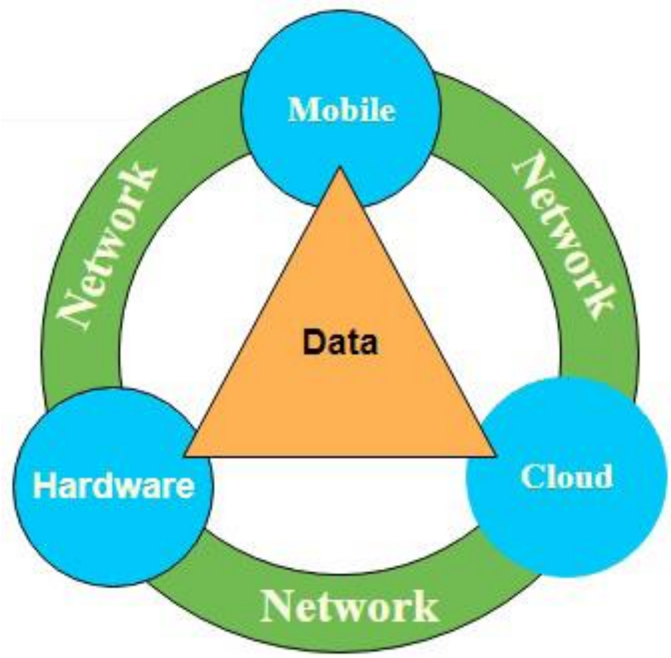

Figure 5.2. The complete IoT product ecosystem.

the platform. Big Data Platform where we can store information get access to it analyze this information ending any useful, industry and industry common trends correlations generate reports. In some cases even control things using an application platform as we may know there are two types of communication one-way communication is let’s say some sensors such as temperature sensor they can only send out information but without talking about communication a real communication is a two-way isn’t it. Sensors send out information to IOT platform and this platform can tell these devices what to do so instead of doing something manually all things will perform automatically. For example we have a Smart Watch and we get into our car our car recognize we are there because our Smart-watch with us. This car can ask our smart house system to set up the comfortable temperature that we prefer and order our favorite pizza by the time we come home and all these things will perform automatically we do not do a single action. So basically we are no longer talking about one way and very dummy almost one-way communication every possible thing will be in internet. In IoT ecosystem there are still some important issues that we should need to be consciously thinking about it. Well understand IoT is how this entire marvelous device is going to be powered actually it is a huge issue and another important thing is what kind of services we can come up with using this IoT platform. How exactly we can provide those for different customers with different requirements using our IoT platform and our wireless networks. So as we can see and understand IoT is not only about particularly technology not only about devices or wireless networks were 5g, big data.

5.2 Setup

In term of IoT make sure all devices have to setup of their suitable device ecosystem. For example where two or more device direct communicate between one another to exchange data than going through an application server in a scenario of a Device to Device Communication (D2D). In D2D communication scenario 6 No Author has given using numerous existing protocols and foundations. D2D may be a promising key development for the time of flexible systems where convenient contraptions set up D2D sessions basic LTE frameworks. Other than, inside the setting of shrewd homes, D2D communication utilizes traditions like Bluetooth, ZigBee or Z-Wave frameworks to set up D2D sessions. This communication demonstrate is commonly utilized in residential mechanization systems where information is traded between gadgets small data bundles with by and large moo data rate necessities. For illustration, in a domestic computerization setup, light bulbs and switches, indoor regulators, entryway locks and conceivably other private gadgets transmit messages to each other [41].

5.3 Functional Testing

When conducting a test on an IoT product ecosystem, to begin with and preeminent an IoT item ought to be set up and designed inside ordinary details. We for the most part favor to set up two isolated situations, which will better facilitate vulnerability testing, such a cross account and cross system attack and can moreover be utilized to create comparisons between typical and modified setups. Leveraging a completely useful environment, able to at that point more viably outline out all capacities, highlights, components and communication ways inside the items ecosystem. Utilizing this data prepared to another build out a test arrange, which covers the things ecosystem from end-to-end. In common, smart home is provide smart services which is run in a home networked that can be run in internally or externally within the home[42].The connected devices interconnected and they are able to share data with one another and they have access to be portion of building automation system (BAS). High-speed Web get to be fundamental for all the devices conveyed within the home to create the IoT. In spite of the truth that the total functionality of a smart home depends on the accessibility of a for all time available Web association where various contraptions can be related within the same occasion to a central center. IoT based BAS grants to control and oversee diverse household contraptions utilizing sensors and actuators such as lighting and shading, security and safety, entertainment, etc [41].

5.4 Open Intelligence Gathering

We begin each IoT security evaluation by conducting reconnaissance and open source intelligence gathering (OSINT) to identify data almost the components and supporting foundation. This identification can incorporate, inquiring about the make and show of the components and computer program utilized by the gadget, and distinguishing proof of any outside nearness that produces up the cloud component of the item. The internet of things developing fast. Helping industry to automate operation and become more efficient to achieve this IoT connectivity must be optimize and reliable. There are many sensors and devices trigger data track from the cloud for some very interactive applications to successful. However there is no alternative to having these round trips of data with extremely low latency. In addition Enterprise IoT data must be kept private requiring robust resilience and secure connectivity for business critical communication. A key technology in this digital transformation is edge computing. A multi access edge computing platform are we call it Mac and rapidly process content at the very edge of the network whether Wireless such LTE like we did in mining environment [44]. Mac enables ultra responsive performance to support augmented reality and other sensitive industrial applications and by keeping track local Mac also ensures enterprise data stays secure and private. For example oil companies can pair real- time drilling data with production data from nearby wealth to automatically adapt their drilling strategy. The efficiency of pipeline and other midstream control system that monitor and provide data from wealth and the pipe itself will be enhanced. Security system like CCTV will be able to transfer video stream at the network edge and send data to remote centers only when anomalies are detected. One two devices reconnecting it and synchronizes its data with a cloud again.

5.5 Capture and Analysis of Data

There's an assortment of information that accessible can be prepared in conjunction with smart connected items. There's outside information coming from outside data sources that may well be accessible as sources through the web. There's endeavor business framework data coming from our CRM frameworks, our ERP frameworks from the framework that we utilize in designing and fabricating. At that point there's information coming from the smart associated item itself. So item data is fundamental to esteem creation and competitive advantage but companies have to be considering a few of the key costs. To begin with there are hard costs like sensors to capture the information. Data transmission expenses on the chance that we push within the information over cellular networks and after that all the capacity required to store the information up within the cloud. Moment is the security and security and hazard moderation around that anything that's associated gets to be a target of programmers and we have a duty very to be

perfectly honest in the event that we collect this information to require great care of it and protect it. At long last there’s a reliance to have the correct set of aptitudes and infrastructure to execution examination and to induce esteem out of data that we are collecting so our proposal is to begin with of all to realize that huge data is exceedingly handled and gadget subordinate and there really is no one size it’s all arrangement. So we think we ought to go to what is our procedure for illustration a technique that’s centered on item execution might have to be to analyze data in real time in order to optimize items or anticipate item downtime on the other hand procedure that’s truly a item framework or framework procedure is progressing to ought to be able to gather numerous sorts of data from numerous diverse sources. So our suggestion would be begin little and attempt to report what are the particular utilize cases over your venture where you'll produce genuine esteem it can be mechanizing consumables or dispatching benefit specialists or performing prescient upkeep and farther diagnostics. So think through those utilize cases and attempt to archive you know what are the most excellent ways and what data we ought to make esteem. At that point we say calibrate the scope of our exertion concurring to a few of the result costs around data transmission and storage. We think as companies develop in their capabilities and in their understanding at that point we are able kind of go back and make changes to our methodology and either collect less data or collect more depending upon the esteem that we have way better understanding. An examination which covers the determination of reasonable reference signals for PEVQ and VQuad-HD can be found within the paper [45].

5.6 Vulnerability Testing of Mobile and Control Application

Concurring to Gartner, the number of Internet-connected gadgets is anticipated to reach 50 billion by 2020. Though IoT is arranging to advance life for various, Within the setting of IoT security, a risk could be a potential to abuse a vulnerability or a potential to violate a security arrangement, and consequently uncover a computer system to harm [46].A few of the common issues which have come up due to the spread of IoT incorporate the following:

- IoT clients grant their endorsement for collection and capacity of information without having satisfactory data or specialized information. Information collected and shared with or misplaced to third parties will inevitably create a point by point picture of our personal lives that clients would never consider sharing with any stranger they met on the street.

- Anonymity has been a consistent issue within the world of IoT, where IoT stages scarcely allow any importance to client anonymity within the prepare of sharing data.

- Cyber attacks are likely to end up a progressively physical (instead of basically virtual) risk. Many Internet-connected apparatuses, such as cameras, tvs sets, and kitchen machines are as of now empowered to spy on individuals in their claim homes. Such gadgets accumulate a parcel of individual information, which gets shared with other gadgets or are held in databases by associations, and they are inclined to being misused.

- Computer-controlled car devices such as horns, brakes, motor, dashboard, and locks are at hazard from programmers who may get to the onboard arrange and control at will, for fun, evil or individual gain.

- The concept of layered security and excess to oversee IoT-related dangers is still in a incipient arranged. For occurrence, the readings of smart health devices to screen a patient's condition may be changed, which once more when associated to another gadget for endorsing drugs post examination, will be compromised, and will unfavorably incense the patient's conclusion or treatment.

- There could be a high probability of disappointment to get access to a special site or database when different IoT-based gadgets attempt interfacing to it, coming about in client disappointment and a drop in revenue.

The IoT innovation frequently uses different sorts of farther control administrations, such as portable applications (Android or iOS), to remotely oversee and control IoT. In this test process, we perform an in-depth test and examination of the versatile and inaccessible applications that are utilized to oversee IoT items. Just like the cloud test, we test all functions of and communications between mobile applications and all components within the IoT item ecosystem to verify the general security state of the product. Moreover, we are going utilize OWASP Top 10 for the center test amid the portable application test. IoT regularly uses standard network communication paths, such as Ethernet and Wi-Fi, to get to different services. Usually helpful but moreover presents numerous risks. In this test stage, we are aiming to distinguish all TCP and UDP ports within the IoT environment framework that are associated to the product. Through these ports, we are able conduct a exhaustive infiltration test to recognize administrations that are powerless to assaults or have setup blunders. Programmers regularly utilize this benefit to vulnerabilities to assault the IoT system and obtain key access information.

5.7 Testing cloud API and Web Services

All back-end stages utilized to trade information with IoT systems, applications, gadgets and sensors ought to be tried to see in case an aggressor is able to pick up unauthorized get to or recover delicate data. These incorporate any outside cloud services (Amazon EC2, Google CE, Sky blue VM) or APIs. Use network graphs, documentation and cloud administration comfort access to evaluate the security of the platforms cloud sending. Evaluate the security design and sending by looking at the taking after major components: key security design plan suspicions, current arrange topology, stock of existing security innovations, security arrangements, rules, and strategies, occasion gather arrangements, organize get to controls, and organize division, remote access and virtual private systems, verification controls counting two-factor verification and single sign-on, data store encryption and key administration, containerization innovations such as Docker and Rocket, and logging and monitoring deployments. Authors in [47] show network engineering and algorithms for ideal determination of interactive media substance conveyance strategies in cloud. Web application testing starts with the organize and working framework to form beyond any doubt the fundamental stages are safely configured. Next, the team will move on to the net application layer - this requires significant consideration and will contain the lion's share of the engagement. For this portion of the pen-test, its vital to play multiple roles: to begin with, as an aggressor without substantial credentials to the internet application, and, besides, as clients who have substantial qualifications. Within the last mentioned occurrence, the testing ought to be conducted over all client parts in arrange to completely look at the apps complicated authorization controls. Apache MLLib and Google Prediction are too accessible to supply forecast functionality on the cloud with actualized libraries and adaptable execution. These stages can be utilized in conjunction with a health event accumulation stage to supply information mining and forecast irregularity administrations for an IoE environment. More detailed data on data analysis on the cloud can be found within the book by Talia et al [48].

5.8 Testing of Embedded Hardware

As the IoT technology develops, consideration is for the most part centered on applications, such as detecting, remote transmission, keenness and other angles of the IoT and overlooking around the fundamental equipment that empowers such functionality [49] .We’ll moreover check IoT gadgets to assess security against the physical layer attacks. Checked objects moreover incorporate gadgets with the JTAG port and serial port, control gadgets of different components, and information and control pins.

In spite of the fact that gadgets have diverse components or arrangements, they have a few common assault vectors, for example:

1. External USB port.
2. Access from external channels.
3. Location and storage media.
4. Access availability of the debug console.
5. Operations required disassembling a device.
6. Risks caused by simple physical access to devices.
7. Risks caused by extended physical access to devices.
8. Risks caused by association media, such as remote association, wired connection, and Bluetooth.

However, lightweights in hardware do not fundamentally infer lightweights in computer program and bad habit versa. Besides, there are indeed plan trade-offs between them [50].

Chapter Six

Discussion

6.1. Discussion

When we engage on doing IoT testing we need to have a standard methodology and the way we approach is fast thing we want to do is identify the full product ecosystem. Regularly this will incorporate mobile cloud equipment additionally the network communication that includes this. Once we have recognized that whole environment we need to focus on setup. The goal is to set up the products entire ecosystem in a full-functioning manner and often we like to set up two independent functioning environments to help facilitate this testing. Once wave done this and we have functionally tested the equipment and ensure that it is working correctly in the way the manufacturer intended to work then we engage and start doing the actual work. The primary thing we need to do is open intelligence gathering. Frequently IoT innovation will use different subsystems which will have a history of having vulnerabilities. We need to recognize that data. We need to distinguish the structure of the IoT innovation as in communication types. How the hardware physically dismantles when was managing with the embedded technology conjointly other communications that would be exterior the typical Ethernet or 802.11 different RF communications. We can often do this by engaging the FCC and use FCC ID information from the actual device. Once wave done that when we want to go on to capturing and analyzing the data communication. What we'll do there is we will set up an environment where we can capture all the communication; we will set up proxy services between the device in the cloud between the mobile application and the cloud. After that well capture and analyze that data for vulnerabilities and issues. Moving from there what we'll do next is well carry out and start doing vulnerability testing of the mobile application. In this case well does a thorough assessment looking for improper authentication poor storage of data, poor communication and a number of vulnerabilities we often encounter mobile technologies? Once that completed well move on to testing the cloud apis. This will test for common cloud vulnerabilities, poor authentication, poor encryption it may also include looking for things like SQL injection, cross-site scripting vulnerabilities. After wave completed that we move on to the last phase of the overall ecosystem. This is the hardware tested in the hardware well actually disassemble the technology well examine it for entry points that may be J tags, it may be UART connections. Well also dig in deeper in the RF communications at this point and try to identify what kind of data is being communicated in that path and is it properly secure also as part of this process. Well attempt to the gain access to the firmware if were unable to get a copy of the firmware via the cloud apis then well often open up the device and actually pull memory, ash memory directly of the device and then well analyzed that for embedded keys, embedded passwords and other issues like undocumented command structure that could be used to carry out further attacks on the device and by focusing on all these key pieces we can identify any security models how they impact each other within our particular proposed model.

Chapter Seven

Conclusions

7.1 Conclusion

Security is increasingly important in IoT. IoT products that were once standalone are now part of a network, increasing both their vulnerability and value. . This model may be appropriate for an IOT device. The other approach is use to a private certificate authority. Essentially having a certificate authority that works in a closed world, so that all the devices that are enrolled with that certificate authority can validate each other using certificates but without reliance on any external third-party. The other factor is that when we go to amazon.com doesn’t use a certificate to validate us. It requires meet the enter our username and password to verify that we are who say we are. In the embedded world when we do machine to machine authentication each device has a certificate so we can do is called mutual authentication. So each device validates the other. Obviously a machine to machine authentication we don’t have a user entering a password or providing biometric authentication so two-way authentication is performed using certificates. For their purposes our proposed IoT testing methodology is very beneficial for IoT industry.

7.2 Future Work

Internet of Things within their enterprises, production facilities are they ready right now to begin introducing smart products and products embedded intelligence. Some recent research was just completed with 350 manufactures across the United States and we think we are finding it really interesting. What we are going to talk about our executive summary of the results is titled the Internet of Things has finally arrived unfortunately are not ready because they are very much off mind about the testing process. Manufacturers are they ready for the Internet of Things? In late 2017 a study of manufacturers in United States and what we found from that research 46 percent of manufacturing executives actually said they had no idea what the Internet of Things was. The fourth industrial revolution (Industry 4.0) enables the integration of information technology with industrial.

Chapter eight

References

8.1 References

[1] Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future generation computer systems* 29, no. 7 (2013): 1645-1660.

[2] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54, no. 15 (2010): 2787-2805.

[3] Miorandi, Daniele, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. "Internet of things: Vision, applications and research challenges." Ad hoc networks 10, no. 7 (2012): 1497-1516.

[4] Aggarwal, Charu C., Naveen Ashish, and Amit Sheth. "The internet of things: A survey from the data-centric perspective." In Managing and mining sensor data, pp. 383-428. Springer, Boston, MA, 2013.

[5] Said, Omar. "Accurate performance evaluation of internet multicast architectures." KSII Transactions on Internet and Information Systems (TIIS) 7, no. 9 (2013): 2194-2212.

[6] Perera, Charith, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. "Context aware computing for the internet of things: A survey." IEEE communications surveys & tutorials 16, no. 1 (2014): 414-454.

[7] Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security for the internet of things: a survey of existing protocols and open research issues." IEEE Communications Surveys & Tutorials 17, no. 3 (2015): 1294-1312.

[8] Sicari, Sabrina, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. "Security, privacy and trust in Internet of Things: The road ahead." Computer networks 76 (2015): 146-164.

[9] Pescatore, John, and Gal Shpantzer. "Securing the internet of things survey." SANS Institute (2014): 1-22.

[10] Gil, David, Antonio Ferrández, Higinio Mora-Mora, and Jesús Peral. "Internet of things: A review of surveys based on context aware intelligent services." Sensors 16, no. 7 (2016): 1069.

[11] Olsson, John Gerhard, and Yuanjing Xu. "Industry 4.0 Adoption in the Manufacturing Process: Multiple case studies of electronic manufacturers and machine manufacturers." (2018).

[12] Blythe, J. M., and S. D. Johnson. "The Consumer Security Index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices." (2018).

[13] Abomhara, Mohamed, and Geir M. Køien. "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks." Journal of Cyber Security 4, no. 1 (2015): 65-88.

[14] Sicari, Sabrina, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. "Security, privacy and trust in Internet of Things: The road ahead." Computer networks 76 (2015): 146-164.

[15] Babar, Sachin, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad. "Proposed security model and threat taxonomy for the Internet of Things (IoT)." In International Conference on Network Security and Applications, pp. 420-429. Springer, Berlin, Heidelberg, 2010.

[16] Wright, Joshua. "Killerbee: practical zigbee exploitation framework." In 11th ToorCon conference, San Diego. 2009.

[17] Stelte, Bjorn, and Gabi Dreo Rodosek. "Thwarting attacks on ZigBee-Removal of the KillerBee stinger." In 2013 9th International Conference on Network and Service Management (CNSM), pp. 219-226. IEEE, 2013.

[18] Tuen, Christian Dancke. "Security in Internet of Things Systems." Master's thesis, NTNU, 2015.

[19] MQTT.org. Frequently asked questions, does mqtt support security? Available at http://mqtt.org/faq.

[20] Lopez, Javier, Ruben Rios, Feng Bao, and Guilin Wang. "Evolving privacy: From sensors to the internet of things." Future Generation Computer Systems 75 (2017): 46-57.

[21] Tonyali, Samet, Kemal Akkaya, Nico Saputro, A. Selcuk Uluagac, and Mehrdad Nojoumian. "Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems." Future Generation Computer Systems 78 (2018): 547-557.

[22] Chen, Xiangqian, Kia Makki, Kang Yen, and Niki Pissinou. "Sensor network security: A survey." IEEE Communications Surveys and Tutorials 11, no. 2 (2009): 52-73.

[23] Krenc, Thomas, Oliver Hohlfeld, and Anja Feldmann. "An internet census taken by an illegal botnet: a qualitative assessment of published measurements." ACM SIGCOMM Computer Communication Review 44, no. 3 (2014): 103-111.

[24] Brody, Paul, and Veena Pureswaran. "Device democracy: Saving the future of the internet of things." IBM, September (2014).

[25] Rauf, Abdul, Riaz Ahmed Shaikh, and Asadullah Shah. "Security and privacy for IoT and fog computing paradigm." In Learning and Technology Conference (L&T), 2018 15th, pp. 96-101. IEEE, 2018.

[26] CAESAR, C. "Competition for authenticated encryption: Security, applicability, and robustness." (2013).

[27] Dunkels, Adam, Luca Mottola, Nicolas Tsiftes, Fredrik Österlind, Joakim Eriksson, and Niclas Finne. "The announcement layer: Beacon coordination for the sensornet stack." In European Conference on Wireless Sensor Networks, pp. 211-226. Springer, Berlin, Heidelberg, 2011.

[28] Ledbetter, William Brian. Analyzing inherent vulnerabilities and associated risks in Bluetooth technology. University of South Alabama, 2017.

[29] Jucker, Stefan. "Securing the constrained application protocol." Institute for Pervasive Computing, Department of Computer Science, ETH Zurich (2012).

[30] Hartke, Klaus, and Olaf Bergmann. "Datagram transport layer security in constrained environments." (2012).

[31] Jankiewicz, Edward, John Loughney, and Thomas Narten. Ipv6 node requirements. No. RFC 6434. 2011.

[32] Varvello, Matteo, Kyle Schomp, David Naylor, Jeremy Blackburn, Alessandro Finamore, and Konstantina Papagiannaki. "Is the web http/2 yet?." In International Conference on Passive and Active Network Measurement, pp. 218-232. Springer, Cham, 2016.

[33] Ryan, Mike. "Bluetooth: With Low Energy Comes Low Security." WOOT 13 (2013): 4-4.

[34] Nieminen, Johanna, Teemu Savolainen, Markus Isomaki, Basavaraj Patil, Zach Shelby, and Carles Gomez. Ipv6 over bluetooth (r) low energy. No. RFC 7668. 2015.

[35] Roman, Rodrigo, Cristina Alcaraz, Javier Lopez, and Nicolas Sklavos. "Key management systems for sensor networks in the context of the Internet of Things." Computers & Electrical Engineering 37, no. 2 (2011): 147-159.

[36] Bos, Joppe, Marcelo Kaihara, Thorsten Kleinjung, Arjen K. Lenstra, and Peter L. Montgomery. On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography. No. EPFL-REPORT-164549. 2009.

[37] Ho, Grant, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song, and David Wagner. "Smart locks: Lessons for securing commodity internet of things devices." In Proceedings of the 11th ACM on Asia conference on computer and communications security, pp. 461-472. ACM, 2016.

[38] Tang, Alexandra, and Jonathan Hytönen. "Digital Lock: Human Detecting Outdoor Lock." (2015).

[39] Akana, Jody, Bartley K. Andre, Shota Aoyagi, Anthony Michael Ashcroft, Jeremy Bataillou, Daniel J. Coster, Daniele De Iuliis et al. "Electronic device with graphical user interface." U.S. Patent Application 29/501,152, filed May 17, 2016.

[40] Mohamed Abomhara and Geir M Kien. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security, 4(1):65{88, 2015.}

[41] Jordi Mongay Batalla, George Mastorakis, Constandinos X Mavromoustakis, and Evangelos Pallis. Beyond the Internet of Things. Springer, 2017.

[42] Yehui Liu. Study on smart home system based on internet of things technology. In Informatics and Management Science IV, pages 73{81. Springer, 2013.

[43] Jordi Mongay Batalla, George Mastorakis, Constandinos X Mavromoustakis, and Evangelos Pallis. Beyond the Internet of Things. Springer, 2017.

[44] Fahim Su, Ibrahim Khalil, and Zahir Tari. A cardiod based technique to identify cardiovascular diseases using mobile phones and body sensors. In Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE, pages 5500{5503. IEEE, 2010.

[45] Christian Hoppe, Robert Manzke, Marcus Rompf, and Tadeus Uhl. Quantifying the suitability of reference signals for the video streaming analysis for iptv. Journal of Telecommunications and Information Technology, 2016.

[46] Mohammed Alhabeeb, Abdullah Almuhaideb, Phu Dung Le, and Bala Srinivasan. Information security threats classication pyramid. In Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference on, pages 208{213. IEEE, 2010.

[47] Yiannos Kryftis, Constandinos X Mavromoustakis, George Mastorakis, Evangelos Pallis, Jordi Mongay Batalla, Joel JPC Rodrigues, Ciprian Dobre, and Georgios Kormentzas. Resource usage prediction algorithms for optimal selection of multi edia content delivery methods. In Communications (ICC), 2015 IEEE International Conference on, pages 5903{5909. IEEE, 2015.}

[48] Alireza Manashty and Janet Light Thompson. Cloud platforms for ioe healthcare context awareness and knowledge sharing. In Beyond the Internet of Things, pages 303{322. Springer, 2017.

[49] Timothy Lee. The hardware enablers for the internet of things{part ii (more than more). Newsletter, 2014, 2014.

[50] Musa G Samaila, Miguel Neto, Diogo AB Fernandes, Mario M Freire, and Pedro RM Inacio. Security challenges of the internet of things. In Beyond the Internet of Things, pages 53{82. Springer, 2017.