Johan Sjölund

Cybersecurity evaluation of IoT systems

Master's thesis
MASTER OF ENGINEERING, CYBERSECURITY

2020

South-Eastern Finland
University of Applied Sciences

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree	Time
Johan Sjölund	Master of Engineering	May 2020

Thesis title

Cybersecurity evaluation of IoT systems

83 pages

Commissioned by

Kybervaliot

Supervisor

Vesa Kankare

Abstract

As the amount of devices connected to Internet is increasing on a daily basis, the need for cybersecurity is now higher than ever and not only the personal computer and server but also Internet-of-things or IoT devices must be protected. While PCs have security software and settings, the IoT devices are lacking in this regard. Hence, the object of this thesis is to gather information about the potential attack surfaces of IoT environment and define guidelines on how to secure an IoT device and/or environment and evaluate an IoT device.

The research was made as a case study, focusing on current issues identified and reported in relation to IoT. The cases used in this thesis are from widely known companies such as Microsoft, F-Secure and OWASP IoT Project.

Based on the cases, the most common issues were selected. The issues were categorized from low to critical depending on the effect the vulnerability might have in case it is exploited. Potential recommendations and guidelines on how to avoid the problems and how to evaluate a device for them.

The conclusion of this study is that there is a high amount of issues. Some of them identified more often than others such as default passwords. Many of the issues are still easily avoidable and solvable while others require more effort but is not impossible to resolve. By following the recommendations from this thesis manufacturers can create more secure IoT devices.

Keywords

IoT, Internet of things, Cyber Security

CONTENTS

1 INTRODUCTION

Cybersecurity is something we can read about on a daily basis in one way or another. Lately, the issues have been related to information leaks (WikiLeaks), computer viruses (Ransomware) or human configuration errors (never changed the default password). With each passing day we are also connecting more and more devices to the Internet, be it computers, smartphones, or even cars, ovens and healthcare devices. We are not only doing this because of the fact that we can but mainly because of our convenience. These items are being connected to the Internet in order to help and improve our lives, work, surroundings and business operations. However, just like computers these devices can expose a risk if they are not maintained and kept secure and safe.

All of these devices are referred under a common acronym, IoT, which stands for Internet-of-Things. According to the Oxford dictionary, the definition of Internet-of-Things is “The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data” (Oxford Living Dictionaries b, 2019). The concept itself, Internet of Things, is old. The first person to use it and hence been given the credit for its invention was Kevin Ashton. According to Ashton, it was first introduced as a title in 1999 for a presentation he made at Procter & Gamble (Ashton, 2009).

1.1 Defining IoT

An IoT device can be an oven which sends the user some data to let the user know when the food in the oven is ready, or it can be a sensor in a car that will inform the driver if there is a problem with the front right tire, for instance. These devices will help us and make our life more convenient. For instance, we can maybe even take it a step further in the car scenario and have the car synced with our calendar and even have the car book a date and time that suits us with a car mechanic without ever having any human interaction.

Another great business example is provided by Deloitte in their “IoT Innovation Report” where in 2015, Amtrack, a US railway company, had issues with their

trains running late. They then turned to Siemens who installed more than 900 sensors along the railway and on the trains to monitor Amtack's equipment. With the help of these sensors, Amtrack was able to spot problems before they occurred, and by the next year, delays were down by one-third (Deloitte, 2018).

Gartner, on the other hand, is predicting that we are going to have over 20 billion Internet-connected devices by the end of 2020 (Gartner, 2017). Another example of further predictions of the amount of IoT devices can be found on Statista website where they predict that up to 30 billion devices will be connected to the Internet by the end of 2020 and 75 billion by the end 2025 as can be seen in Figure 1 below.

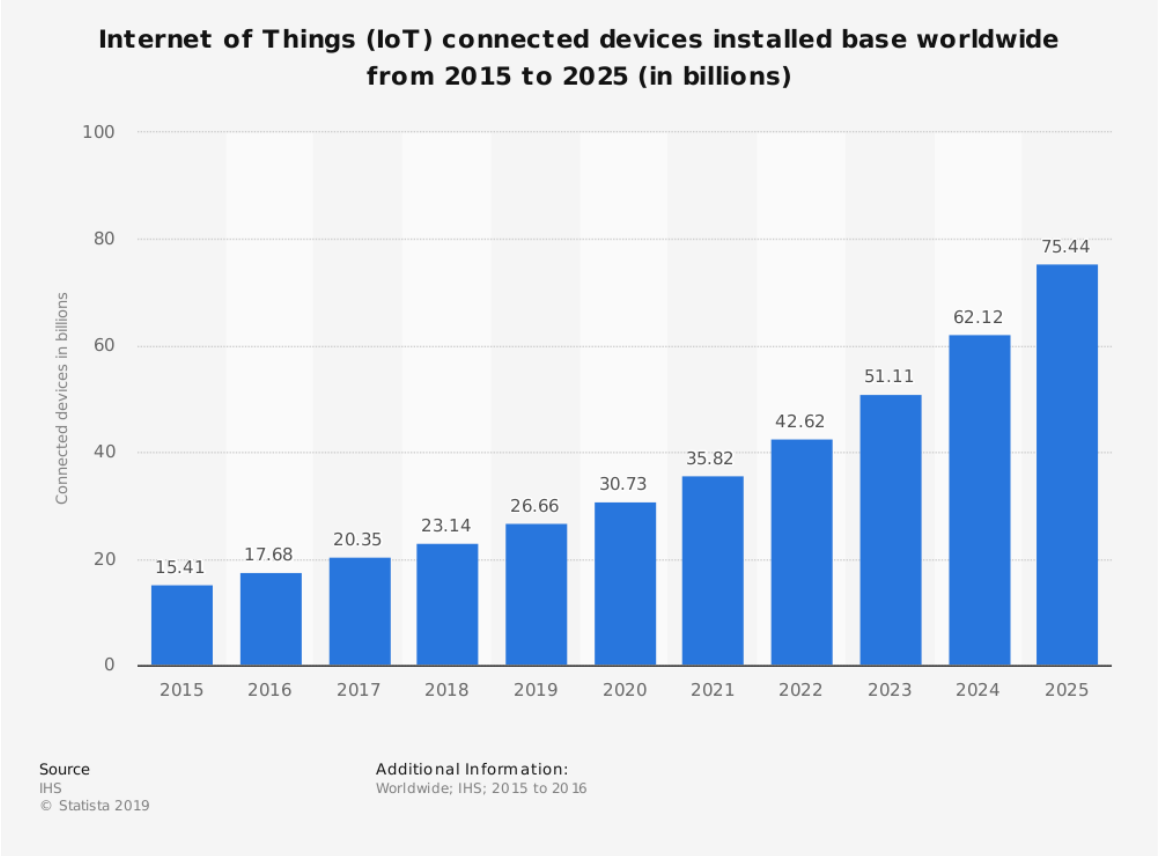

Figure 1. IoT connected devices (Statista, 2016)

However, when it comes to the security perspective of IoT devices, there are great of concerns. Connecting an IoT device to a home network is not simply plug-and-play procedure as some customers might believe. One needs to configure it, update it if needed and even know when it might be time to retire the

device. This means that some IoT devices stop receiving updates after a while due to age or hardware issue, so that the security issues they are facing at that point will never be fixed.

An example of an issue that can be easily fixed is the hard-coded default passwords on the devices. They are seldom flawless and can usually be easily found with the help of Google. Unless the users themselves change them, if that is even possible, and these devices face the threat of being accessed by third parties. An easy solution to this would be to enforce an installation process which requires the users to change the password during the installation/setup phase.

Another example of a poorly designed IoT device is the toy CloudsPets. According to Tara Seals at Threatpost.com (2018), these little cuddly teddy bears and unicorns were able send and receive messages via a smartphone app. The idea was to let the parents communicate with their kids through these toys which, as such, was a nice idea. However, these messages were not secured, and a hacker managed to get access to them. Other issues were later found as well (Tara Seals, 2018). This led to resellers such as Amazon having to pull them off the shelves. However, even today, 2019 one can still find these CloudPets unicorn on eBay for around 27€. The smartphone app, however, could not be found in the iPhone app store, but several websites still have it available.

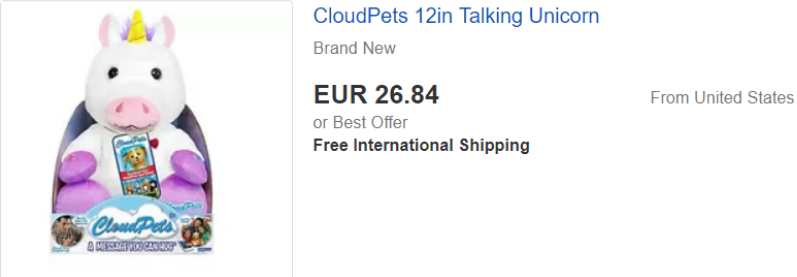

Figure 2. Screenshot from eBay (eBay 2019)

This device, of course, is not something that would very likely be found in a business environment or could very easily harm someone but serve as an example of how some IoT devices do not necessarily have the best security features and illustrate the fact that these such defective are still being sold. One

reason for this might be that there are no strict rules in the world of IoT security, and today it is easier than ever to create new devices. According to Tom Gaffney from F-Secure, anyone with an idea and basic programming skills can quite easily start working on an IoT device, even people that do not necessary understand security (Gaffney, 2019).

1.2 IoT environment

What needs to be carefully considered is the whole system behind the devices and not only the IoT devices themselves such as network and servers. A common and yet simple setup of an IoT system could look like something like this drawing done by IBM (IBM, 2015)

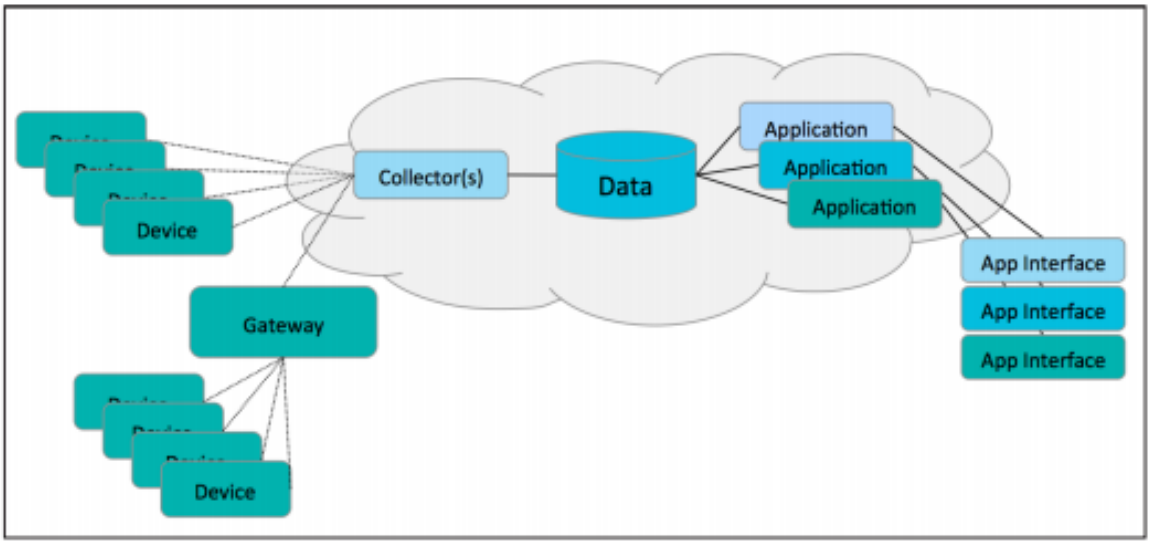

Figure 3. IoT System (IBM 2015)

As can been seen in Figure 3 and Figure 4, there are several devices that are either directly in contact with a collector or through a gateway meant for device management. The collector shares the data it receives with the applications which in return are connected to an application (app) interface, for instance, to a smartphone, that allows the users to see and control the device(s) based on the data they receive. An example of such, turning on or off lights (the devices) that are connected to a hub (the gateway) that is controlled through an app on a smartphone.

Another example of an IoT environment can be found in the documentation created by Lawrence Miller. Miller's diagram for a standard IoT environment can be seen in Figure 4.

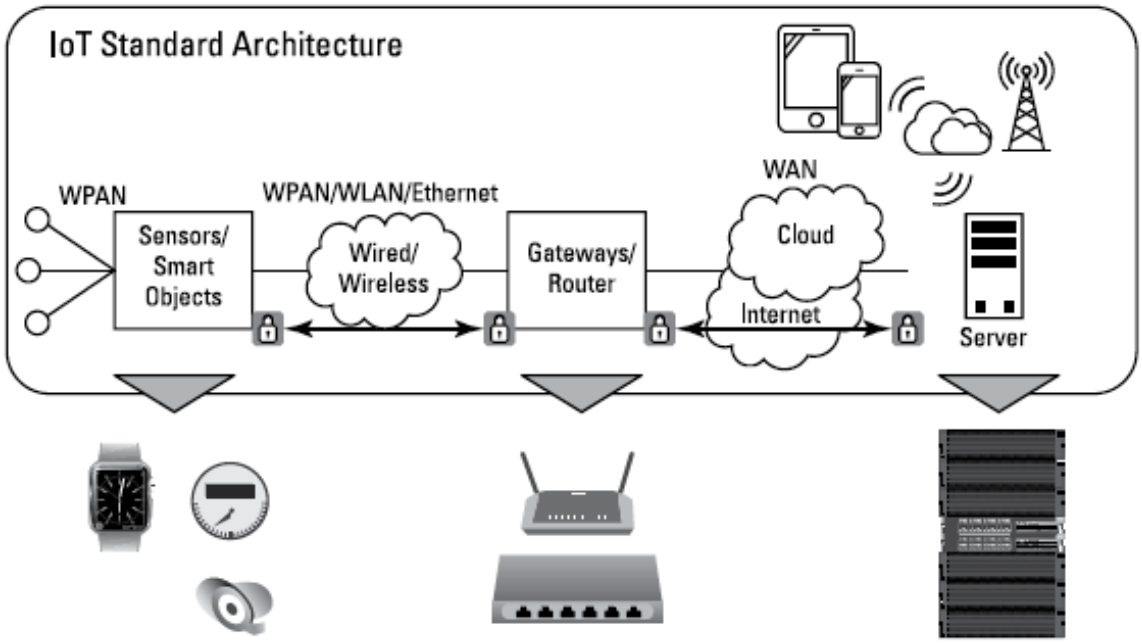

Figure 4. Standard IoT Environment (Miller, L 2016)

In Figure 4 one can see the standard devices found in an IoT environment. In this illustration, sensors/smart objects communicate over a wired/wireless network with a Gateway/Router which in return is in contact with a server which is usually located in the cloud. The server then presents the data gathered with the help of the sensors to the end users' mobile phone application. Miller also created a simple diagram for a how a sensor could look like (Figure 5).

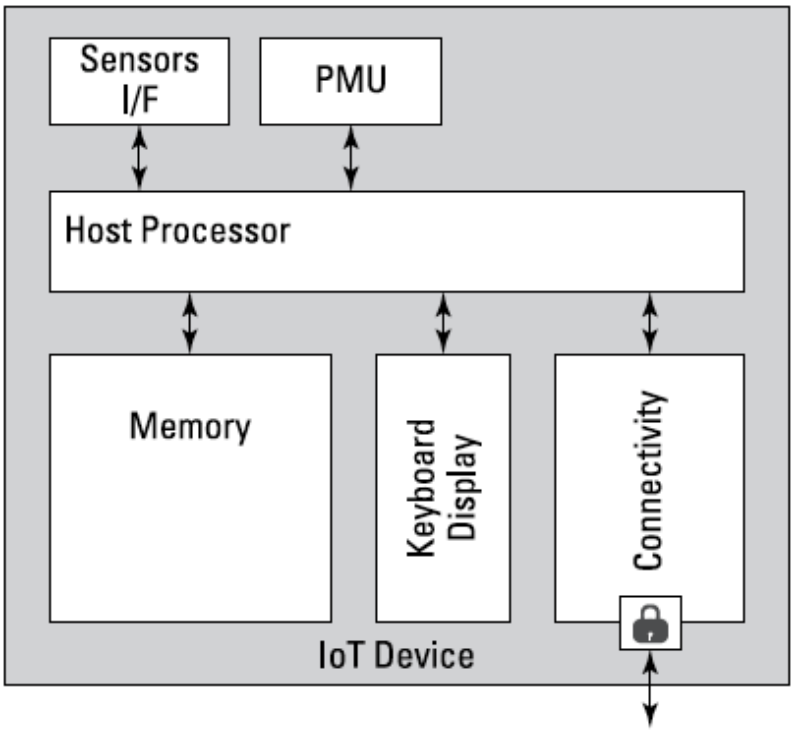

Figure 5. Standard IoT Sensor (Miller, L 2016)

A sensor usually consists of the following devices:

- Sensor Interface which collects the data
- Power management unit (PMU) to turn off and on the device
- Host processer which acts as the brain
- Memory to store the collected data and configurations
- Keyboard/display which Miller describes as “the man-machine interface”
- Connectivity for communication, which could be over wired or wireless ethernet, Bluetooth.

1.2.1 Potential risks related to IoT

All devices listed by Miller and discussed in the previous chapter are a part of the IoT environment but at the same time they are also potential surfaces for attacks, depending on what kind of access a hacker has to either the IoT environment, network or the device itself.

Depending on where the device is and how it works, a hacker can potentially have physical access to the device and download the configuration from the

memory of the IoT device. If the device is Internet facing, the hacker could potentially access the device by knowing or discovering the IP address of the device. After that, the hacker could access the device over the Internet. These are simply a few examples and Miller points out that security is like a chain, it is only as strong as its weakest link (Miller 2016). In other words, even if the best security is placed on the IoT device and app, it does not help if the server is unsecured or the data sent to the server is unsecured and third parties can read it.

Daniel Miessler, of OWASP IoT project, held a talk on Def Con 23 about IoT Attack Surface Mapping and pointed out that IoT security does not mean the physical security of the device itself. It should involve the whole IoT environment and Miessler also commented that this is one of the issues in the IoT world today (Miessler, 2015).

1.2.2 Protection of different IoT environments

According to Miller, with all the new IoT environments that are supposed to make our lives easier and more convenient comes also major challenges (Miller 2016). IoT devices collect great amount of personal data, potentially also financial or personal health information that can end up in the wrong hands if manufacturers do not have the appropriate security controls in place.

As can be seen in Figure 6, Miller has also created a diagram depicting four areas of how an attack can affect the IoT environment.

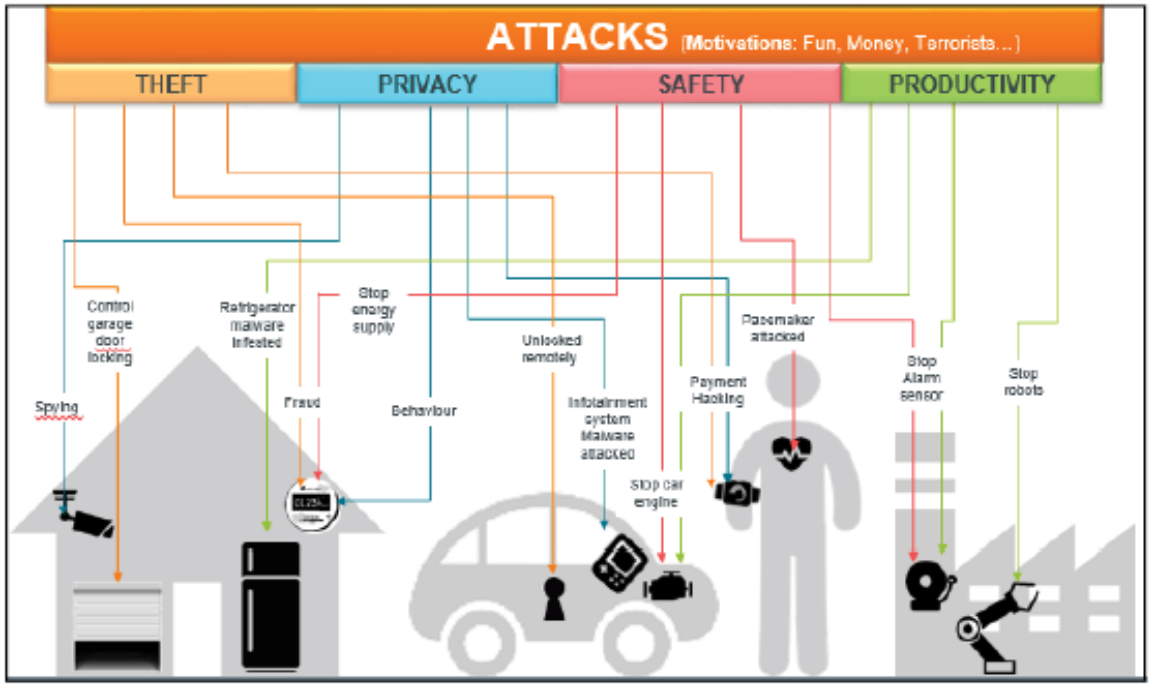

Figure 6. IoT Security for Dummies (Miller, L 2016)

The four areas, as presented in Figure 6, are explained as follows (Miller, 2016):

- Theft extends beyond just credit cards and identities. A hacker can potentially open the door to a person's home and steal physical valuables as well, if an IoT lock is in use.
- Private data is usually stored in the cloud and it can contain everything from biometrics and health information to personal behaviour, eating habits and locations. If an attacker got their hands on this data, they would be able to check if a person is at home or out for a run.
- Safety is referring to actual physical safety of the users. An attacker can potentially get access to a health meter or insulin pumps and adjust how they work or maybe tamper with the breaks on a car.
- Productivity is a business perspective. An attack could alter robots on the production line or tamper with fire alarms or air conditioning to cause other expensive interruptions.

Miller points out that by securing the IoT devices and eliminating their associated theft, privacy, safety and productivity security risks, manufacturers protect their own business and their reputation as well. Miller also mentions that a cost of a security breach depends on many different reasons, but Verizon provided a

report in 2015, which stated that a breach of 100,000 records has a cost of approximately $474,600 (Verizon, 2015). This sum included direct costs such as actual damages, fines, litigation and remediation. Indirect damages such as damages to the reputation or the loss of potential future customers or current customers.

1.2.3 IoT devices in different sectors of work

There are no clear regulations yet on what is needed to create an IoT device today, so security may vary from almost non-existing to something that is being developed on a daily basis by the manufactures. Depending on the environment, some IoT devices are better suited for home use rather than government use but that is entirely up to the customers.

An example of an IoT device which is generally seen as a good device and can be found all around the world these days are fitbands or smartwatches. They help the wearers track training and fitness among other things. Buying and using these devices will mean that the user usually needs to provide information such as GPS locations so that the device can track activities or act as a step counter. There is even an application that gathers this information and then allows the user to share this information with friends and family and in some cases the “Internet”.

There could be problem when these trackers and applications are used by Military personnel. The movement will be tracked in the same way. If these devices are used as step counters with GPS tracking turned on, patterns can quickly start appearing. This happened with the Strava fitness app which had an option to create a heat map tracking which lead to military guard patterns and training patterns showing up on the application world map which can be seen in Figure 7.

Figure 7. A military base in Helmand Province, Afghanistan with route taken by joggers highlighted by Strava (The Guardian, 2019)

The Guardian reported about this incident in January of 2018, and also added that according to Nathan Ruser, who detected this issue, US army bases were made clearly identifiable and mappable due to the heat map features in the Strava app (Hern, 2018). After this incident, Strava has urged military personnel to opt-out from heat map feature.

1.2.4 End of life scenarios for IoT

In some cases, IoT devices are forced into early retirement due to support stopped for them. In IT world, this scenario is often referred to as end of life, or EoL. This might be a huge problem for people who have bought many devices which suddenly stop receiving support. However, this phenomenon is not that uncommon in the IT world. Companies stop maintaining old devices and systems in order to move forward with the use of other and newer devices and systems. A good example of this in is all the different Windows operating systems that have been retired in order to make way for the newer and more secure versions of the systems.

This also happens in the IoT world. IoT devices stop receiving updates from the manufacturer as they want to push forward with newer, and potentially better, devices and hence force the users into buying the newer versions of the IoT devices if they want to feel safe and secure. The users may also have the option

to accept the fact that their devices do not receive any more updates and could potentially be at risk. One good example of this is Google Nest, which acquired Revolv in October 2014 which sold a smart home hub for approximately 300 US dollars (Price, 2016). In May 2016, the Revolv website was updated with an announcement stating that they would be shutting down, meaning no more maintenance will be provided for the devices their customers had bought, which of course disappointed many them. Other issues that might occur is that the manufacturers may go bankrupt causing the support for the device to stop, as was seen in the CloudPets example earlier.

1.3 Defining Cybersecurity

According to the Oxford dictionary, cybersecurity is “the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this” (Oxford Living Dictionaries a, 2019). In other words, it is the act of protecting any kind of a system containing data from an attack. However, keeping the data safe is not the only thing which is related to cybersecurity. One must also try to keep the devices themselves secure. Otherwise it would be extremely difficult to define whether or not the data is authentic (unchanged) or not.

The best way in make sure the data is safe is by maintaining the CIA, Confidentiality, Integrity and Availability, triad of cybersecurity. These are simple and useful points to remember and are usually the targets of a cybersecurity attack.

1.3.1 CIA Triad

As mentioned earlier, the CIA triad, consists of Confidentiality, Integrity and Availability and cybersecurity aims to maintain these three all time. According to Forcepoint, it is important to understand the CIA triad and the ways used to implement quality security controls and understand the principles (Forcepoint, 2019).

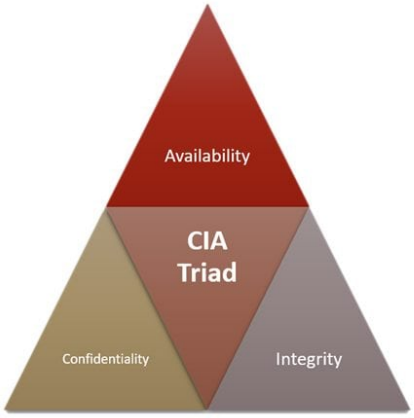

Figure 8. CIA Triad (INFOSEC, 2018)

1.3.2 Confidentiality

Confidentiality refers to the act of establishing who has access to the data. It should be based on the need to know basis (INFOSEC, 2018) as there is no need for everybody in a company to have access to all the information the company has. For instance, human resources do not need access to the network equipment while IT does, and IT does not need access to personnel information which human resources does. At the core of confidentiality is a strong data classification policy in which ables to classify the data. Once that is in place, one can determine who should have access to what data and why.

1.3.3 Integrity

Integrity is the act of making sure data is not tampered with either during transfer from source to destination or in rested state. Information should be protected by access control during rested state and by encryption during transfer in order to prevent an external source from tampering or accessing the data (INFOSEC, 2018).

1.3.4 Availability

The goal is of availability is making sure the information is available at all time. That might sound simple enough but in today's world there are plenty of Distributed Denial of Service attacks, DDoS, which usually do not have any other

purpose than bringing down a service (INFOSEC, 2018). An example of this is the DDoS attacks against Sony and Microsoft during Christmas of 2014 when their networks were attacked by the hacker group Lizard Squad only to cause disturbance (Kiss, 2014).

1.3.5 The need of cybersecurity

The world uses more and more technology every day. According to Gartner, there are estimates of over 20 billion devices connected to the Internet by the year 2020 (Gartner, 2017). Along with the devices comes also plenty of information that needs to be maintained, monitored and protected.

All devices contain data in some form that is valuable to someone. Some of the data might be personal and has no value to anyone except to the owner, for instance family photos. Other data such as browser history, credit card history or, even worse, card details have great value in the world of corporate espionage or credit card details that can be sold. A data breach can cause grave concerns and have grave consequences for a company, be it a cloud storage provider getting hacked and customers losing access to their pictures or stealing the customer's credit card details they have been using to pay for the service. A worst-case scenario for the storage provider is that everybody stops using their service as the customers have lost faith in the provider to keep their data safe and secure.

With the help of cybersecurity, one can try to minimize these scenarios and possibilities where all the data or some of the data is stolen. Stopping these scenarios completely is very challenging as too many factors can be involved. One needs to remember that an attacker only needs to correct once in order to get access. Cybersecurity, however, will help avoid and limit the damage that can be done through a breach if it was to happen.

1.3.6 Different types of cybersecurity

There are plenty of different types of cybersecurity devices and approaches to improve security at an organization. The following section provides a few examples of devices and approaches that improve security.

Network security aims to help protect the network with the help of physical Firewalls, Intrusions Detection Systems (IDS) and Intrusion Prevention Systems (IPS) for instance. Application solutions like Antivirus software protect both PCs and Macs against viruses and spyware and, finally, then there is application Firewalls no name a few examples.

Limited access which is based on the “C” in CIA triad which in turn means that access towards information should only be provided on a need-to-know basis. Again, this is more information security rather than cybersecurity, but one thing can lead to another.

Awareness training is another type. It focuses on providing the users with the knowledge of the most common issues. Security software will never replace the people using the machines and is there to aid the users and not act on their own and serve as a means of defence. Related to the awareness training, one can also do internal tests to make sure that the users are following the instructions from the training sessions.

1.3.7 Different forms of threats

Similarly to the different forms of cybersecurity, there are also many different types of threats. The following section is focused on a few examples and scenarios.

An angry employee scenario is something that can happen to anyone. The damage that can be caused can vary on range from minor to major. The employee can steal information in order to sell it for personal gain, for instance, but with the help of CIA triad this type of threat can be limited by only allowing

employees access to the information they need. The workers of human resources, do not need to know classified project information.

Phishing emails are attacks that ask users for their credentials or telling them the sender is from their local IT support or that they have won a competition and need to fill out a form or by sending them malware.

Distributed Denial of Service (DDoS) only aim to cause a disruption in a service by flooding a target with so many requests that it cannot process anymore. This in return might lead to the whole system crashing if the right service is targeted. An example of this would be Lizard Squad attack on Sony and Microsoft that was mentioned before.

Finally, zero-day exploits. Zero-day exploits are exploits that have not been revealed yet. The exploit can be a bug in Windows which gives the attacker administration rights to the device. Once these exploits have been revealed, which means in some cases they have been used, they can be patched by Microsoft but until then they remain undetected and can cause potentially damages.

2 OBJECTIVE OF THE STUDY

The object of this thesis is to provide a set of guidelines and rules to help manufacturers implement and improve the security of the IoT devices so that they can protect the users, the data and the IoT devices. Even if an IoT device might have some security, the problem is that it is limited.

2.1 Research questions

The questions this study will try to answer are the following:

- What attack surfaces can be identified in IoT systems?
- What methods are suitable to evaluate the cybersecurity of IoT systems?

By answering these questions, the study aims to define the most common flaws in an IoT environment in order to mitigate attacks against an IoT system. Once

the most common attacks are defined, one will be able to evaluate them and try to find a solution, hence minimizing the potential attack surface.

2.2 Research method

In order to achieve the object of this thesis a research method needs to be chosen. There are three options when it comes to choosing a research method. It can either be qualitative, which focuses around producing new knowledge, or it can be quantitative, which is often uses data from existing researches (Kananen, 2015). The third option is a blend of the two earlier mentioned. This study will be a blend between the quantitative and the qualitative method. With the help of combining these two methods a case research can be done. In a case research, the researcher himself does not participate. He only acts as an observer. A case research does not necessarily aim to change anything but to understand and explain a phenomenon (Kananen, 2015). Since the objective is to understand current issues in the IoT environment, a case study should prove beneficial.

In this thesis, the case study will be done using cases from real life scenarios. With the aim of demonstrating how an IoT environment, not simply the devices themselves, could be protected within reasonable effort and budget. As with any scenario in the security world, risk management is extremely important.

The aim of the study is to gather data from known vulnerabilities, issues and weaknesses in the IoT environment. The study also gathers information about existing best practices. Based on this, a set of recommendations and possible solutions on how to improve an IoT environment in order to protect users, data and the devices will be presented.

3 CASE STUDY

3.1 US Government Bill, Cybersecurity Improvement Act

As mentioned earlier, IoT devices and environments have existed for a long time and the term itself was introduced in 1999 by Kevin Ashton. However, required or recommended security has not improved too much since that date, but one can

see a change in that now. For instance, the U.S Senate and House of Representatives introduced the “Internet of things (IoT) Cybersecurity Improvement Act of 2019” as reported by the CISO Mag (CISOMAG, 2019). The intention of this bill is to make sure that IoT devices purchased by the U.S government meet a set minimum of security requirements (CISOMAG, 2019).

Along with the introduction of the bill there was also a press release from senator Maggie Hassan stating some of the issues seen in the IoT environments today. The release said that, sometimes IoT devices are shipped with factory-set, hardcoded passwords and are unable to be updated or patched. IoT devices can represent a weak point in a network’s security (Hassan, 2019).

The bill aims to do the following (Hassan, 2019):

- Require the National Institute of Standards and Technology, NIST for short, to issue recommendations that addresses secure development, identity management, patching and configuration management of IoT device.
- Charge Office of Management and Budget, OMB, to guidelines and review the policies every five years
- Require any Internet-connected device bought by the government to comply with the NIST recommendations.
- Direct NIST to work with cybersecurity researchers and industry experts to publish guidance on coordinated vulnerability disclosures to ensure that vulnerabilities are addressed.
- Require that contractors and vendors that are providing IoT devices to the U.S government adopt coordinated vulnerability disclosure policies, so that if a vulnerability is discovered the information is shared with everyone involved.

This means that in the future, if this is bill is made into law, whenever IoT manufacturers are interested in selling to the U.S government, they need to comply to this bill. Also, in the interest of making things easier, consumer devices might come with the same set of rules and guidelines instead of having one set of

IoT devices for the U.S government and one set for consumers, which would benefit the whole IoT world.

Jeff Greene, Vice President of Global Government Affairs and Policy at Symantec said that IoT devices are a risk one must address. It will only happen if the government and the private sector both step up (Hassan, 2019).

Furthermore, this bill is also supported by Rapid7 (Cybersecurity company), CTIA (represents the U.S wireless communication industry) and Tenable (Cybersecurity company) (Hassan, 2019).

The U.S Senate also tried introducing a similar bill like the Internet of things (IoT) Cybersecurity Improvement Act of 2019 in 2017 called Internet of things (IoT) Cybersecurity Improvement Act of 2017 but it was never enacted on that is it was never made into a law (Gallo, 2019).

3.2 NIST's Guidelines and Recommendations

NIST, which stands for National Institute of Standards and Technology, has also released their own set of recommendation regarding IoT devices and environments. NIST was founded in 1901 and is now a part of the U.S Department of Commerce. It was established to remove major challenges to U.S industrial competitiveness at the time. Today, NIST supports a wide range of devices, from the smallest of technologies to the largest and most complex devices (NIST, 2017).

As mentioned earlier, when there is a need for guidance, the U.S government turns to NIST, regarding upcoming IoT requirements. July of 2019 NIST released in a set of guidelines, not rules, in their report Core Cybersecurity feature baseline for securable IoT Devices (NISTIR 8259) that is intended for IoT device manufactures. They also released Considerations for managing Internet of Things (IoT) Cybersecurity and Privacy Risks (NISTIR 8228) report which was meant to aid IoT device customers to understand the potential risks and challenges with IoT devices.

3.2.1 NIST Security Feature Recommendation for IoT devices

The NISTIR 8259 report is intended to help manufacturers to meet the bare minimal security needed to keep the IoT devices and environments safe and secure. In NISTs own words, the core baseline is to help the customers (manufactures) achieve a basic cyber security posture that mitigates general cybersecurity risks. By including these bare minimal, manufacturers help enable IoT device consumers to effectively manage their cybersecurity risks (NIST, 2019).

NIST has established three high-level considerations that may affect the management of IoT devices from a cybersecurity and privacy perspective compared to the conventional IT devices such as laptops or servers. These three areas are (NIST, 2019):

1. **Many IoT devices interact with the physical world in ways conventional IT devices do not** - meaning that they can make physical changes to the physical world (industrial control systems like robots for instance). This needs to be recognized and addressed from a cybersecurity perspective. Operational requirements for performance, reliability, resilience and safety also needs to be taken into consideration.
2. **Many IoT devices cannot be accessed, managed or monitored in the same way other conventional IT devices can be** – meaning users cannot for instance install antivirus software on the IoT devices in order to add an extra layer of security on them.
3. **The availability, efficiency and effectiveness of cybersecurity features are often different for IoT devices compare to other conventional IT devices** - this means that users might have to install, manage and maintain additional devices, IoT or others, as well to be able to respond to risks when sufficient controls for risk mitigation is not available.

NIST also stated that, from a cybersecurity and privacy perspective, IoT device manufacturers should have these three following goals in mind when they are planning IoT device security (NIST, 2019):

a. **Protect device security** – prevent the device from being used to conduct attacks, being a part of botnets and DDOS attacks,

eavesdropping on traffic or compromising other devices on the same network segment.

b. **Protect data security** – maintain the CIA of the data collected, stored, processed and transmitted by the IoT device.
c. **Protect individuals' privacy** - protect personally identifiable information (PII) collected by the devices.

Each of the objectives complement each other and do not negate the need for the previous objective or objective s. Meeting each of the risk mitigation objectives means addressing a set of risk mitigation areas which are the following (NIST, 2019):

Risk mitigation areas for Device Security:

1. **Asset Management** – maintain an up to date list of current known IoT devices, whether they are in use, in stock, in repair or even retired throughout the lifecycles.
2. **Vulnerability Management** – identify and remove known vulnerabilities in both the software and firmware in order to reduce the likelihood of miss use the of the devices.
3. **Access Management** – maintain strict access to the IoT devices both physical and logical so that only authorized personnel can access them
4. **Incident Detection** – have systems in place that can monitor the IoT devices activity for any signs of miss use and data security.

Risk mitigation areas for Data Security:

1. **Data Protection** – prevent tampering with the data in anyway.
2. **Incident Detection** – have systems in place that can monitor the IoT devices activity for any signs of miss use and data security.

Risk mitigation areas for Individual Privacy:

1. **Information Flow Management** – maintain a current and accurate information lifecycle of the personally identifiable information (PII).
2. **PII Processing Permissions Management** – maintain permissions for PII.
3. **Informed Decision Making** - enable users to understand the effects of PII processing and interactions with the IoT devices.
4. **Disassociated Data Management** - Identify authorized PII processing and determine how PII mat be minimized or disassociated from the user and IoT devices.
5. **Privacy Breach Detection** – monitor for signs of breaches involving individual's privacy.

3.2.2 NIST IoT management issues

According to NIST, many IoT devices are often called “black boxes” because they provide little or no information about their state and composition report “Considerations for Managing Internet of Things”. The users may not know what the IoT devices are capable of hence NIST created the report IR 8228 to help users protect themselves. The report is targeted towards federal agencies and large corporate businesses rather than home users but that does not mean that the home users, still could not have any use of the report. (NIST, 2019)

Authorized people, processes, and devices may encounter one or more of the following challenges when trying to access, manage, and/or monitor the IoT devices: (NIST, 2019):

- **Lack of management features** – users are not able to fully manage an IoT device’s firmware, Operating System (OS) and applications throughout the lifecycle of the device so installing or updating the devices is not always possible. In addition to this, in some cases IoT devices can be automatically reconfigured in the event of power failure or loss of connectivity.
- **Lack of interfaces** – some IoT devices lack application and/or human interfaces for device use and management.
- **Difficulties with management at scale** – most IoT devices do not have the support for centralized management.
- **Wide variety of software to manage** – This complicates software management throughout the IoT devices lifecycle.
- **Differing lifespan expectations** – a manufacturer may intend for a particular IoT device only be used to a few years and then wish to retire them. However, users might want to continue using them longer and by then the manufacturers have stopped supporting the devices meaning all the vulnerabilities will never be patched.
- **Unserviceable hardware** – the devices cannot be repaired, customized or inspected internally.
- **Lack of inventory capabilities** - IoT devices brought into an organization may not be inventoried via the normal IT processes.
- **Heterogenous ownership** – sometimes there is a “mixed ownership” of the devices. Some IoT devices manufacturers will remain in control of the devices regarding patch management, troubleshooting and other installations. Then there is also data that in many cases are being sent to the cloud meaning that the cloud providers have access to it and in some case even access control of the IoT devices. Another concern with these kinds of “mixed ownerships” are the possibilities of reprovision the devices.

These issues and challenges all affect the possibilities of achieving the three objectives set by NIST to maintain a secure IoT environment, even if it is only a printer in the office or at home.

3.3 EU Cybersecurity Act

In the EU, there is a similar law that was adopted on the 12 of March 2019 titled the EU Cybersecurity Act and it has been in effect since 27 of June 2019. In short, the Cybersecurity Act aims to strengthen the European Union Agency for Network and Information Security (ENISA) in its roll to support the EU to achieve a common high level of cybersecurity. It also seeks to establish the first EU-wide cybersecurity certification framework to make sure that there is a common cybersecurity certification approach in the wide and broad range of digital products, among them IoT devices, and services (European Commission, 2019).

In addition to the IoT changes, the EU Cybersecurity Act tries to encourage manufacturers to implement security measurements at the earliest stage possible. Security should be a part of the product design and not simply an afterthought applied only because there should be one. These security measurements should also be a part of the product's lifetime and constantly evolving to reduce the risk of malicious exploitations (Council of the European Union, 2018). Also, the EU Cybersecurity Act wants to make manufacturers aware that security procedures should not require extensive configuration or any specific technical understanding.

The General Data Protection Regulation (GDPR), which has been in effect since May the 25 2018, which per say does not regulate IoT devices per se but monitors personal data gathering. The objective is to help the customers get control of their data collected by services and also provide a greater insight into the data collection and the use of the data (Core DNA, 2019). This could and should also be kept in mind when designing IoT devices as many of the devices gather in one form or another this kind of data.

3.4 ENISA

As part of the EU Cybersecurity Act, the EU wants to provide more power to ENISA in order to create a framework for IoT devices. As of today, ENISA has already released guidelines with the objective to advice and sets recommendations on good practice in information security for the countries of the EU (ENISA, 2017). The current guidelines published by ENISA are from November of 2017 in the report “Baseline Security Recommendations for IoT”, which as the name reflects, contains recommendations for IoT devices.

According to this report, the security of IoT should be made a fundamental priority as the IoT devices can affect people’s security, privacy and safety and can additionally be used as an attack vector against other infrastructure devices. Also, the adoption of IoT has raised many legal, political and regulatory challenges also according to ENISA. The rate of changes in the IoT world is also causing issues as they outpace the ability to regulate the devices which in return has led to companies using their own approaches instead of common solutions (ENISA, 2017).

For this reason, ENISA has created a set of Baseline Security Recommendations for IoT. The objective with the report is to provide insight into the security requirements of IoT, mapping critical assets and relevant threats, assessing possible attacks and identifying good practices to protect the IoT environment (ENISA, 2017).

3.4.1 ENISA critical attack scenarios

In order to get a better understanding of some key risks and threats in the IoT environment, ENISA conducted interviews with experts and key stakeholders discuss three potential attack scenarios. They focused and on the top three issues which can been seen in Figure 9.

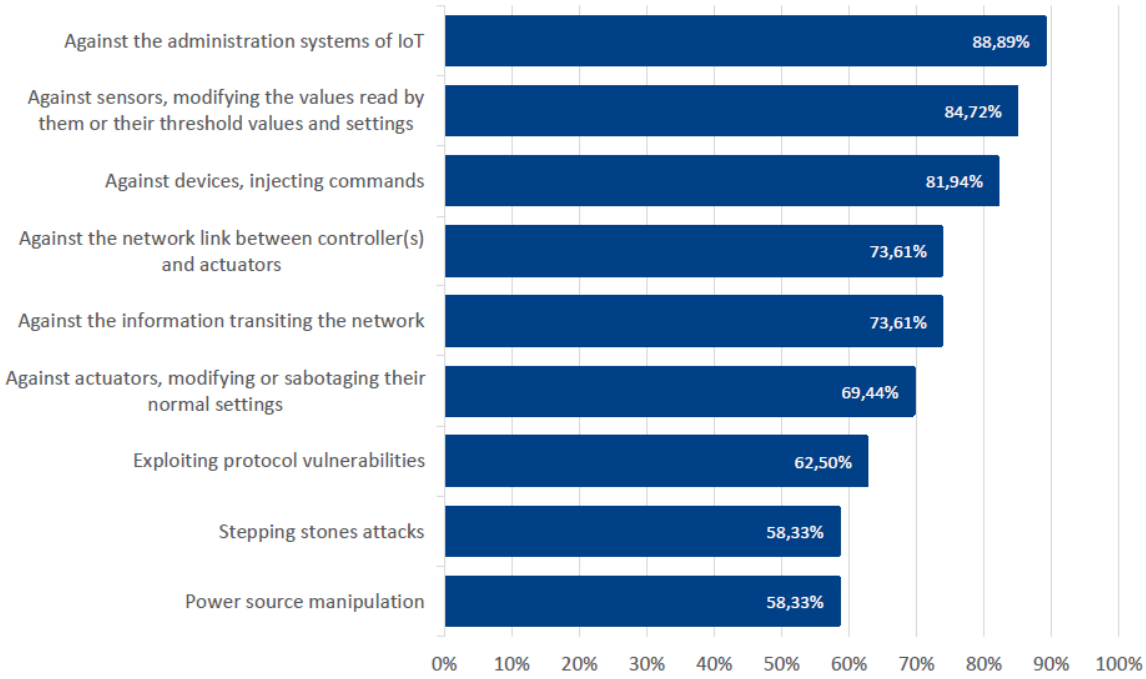

Figure 9. The attack scenarios criticality (ENISA, 2017)

3.4.2 Attack scenario 1 – IoT administration system compromise

The attack starts with gathering of information about the network and different IoT devices. Once the IoT devices have been identified, the attacker gathers information about known vulnerabilities and exploits them. Once compromised, a back door is installed to maintain presence in the network. After this, the attacker only needs to modify the system to permanently compromised (ENISA, 2017).

This way, an attacker can gain full control of the device. It is possible to see all the data the device is gathering and have to access the device whenever (ENISA, 2017).

3.4.3 Attack scenario 2 – Value manipulation in IoT devices

This attack starts with setting up an IoT device such as a sensor or a robot. All the configurations are stored locally in the system and since the data is stored locally an attacker can manipulate the values causing the device to act unexpectedly.

It is important to remember that this scenario could happen to an ICS in a car factory, which might put people's life's in danger or cause physical damages to property (ENISA, 2017).

3.4.4 Attack scenario 3 – Botnet / Commands Injections

This attack is based on Mirai botnet which has conducted several successful DDOS attacks and including some most forceful ones as well to date. The attacker starts with scanning for open ports on IoT devices accessible over the Internet. The reason for this is they are usually poorly protected by default usernames and passwords. The attacker will then inject commands into the device's console in order to obtain administrator privileges. If this is successful, the attacker will connect the device to a command and control server under their control to download malicious scripts. The scripts will execute and delete itself afterwards and run in-memory. Once that is done, the bot will spread and start attacking in the same way other vulnerable devices in order to build up an army of IoT devices which the attacker controls from the command and control server in order to launch DDOS attacks (ENISA, 2017).

The impact of these kinds of attacks may vary by a lot as it all depends on the criticality of the target and the number of IoT devices which are part of the botnet (ENISA, 2017).

3.4.5 ENISA Recommendations

The ENISA list aims to improve gaps they found rather than recommend direct actions (ENISA, 2017).

1. Promote harmonization of IoT security initiatives and regulations – define guidelines for security and privacy which can be used for development of IoT systems.
2. Raise awareness for the need for IoT cybersecurity – raise awareness among all involved in the IoT world by training.
3. Define secure software/hardware development lifecycle guidelines for IoT – integrate and process for a secure software development lifecycle, meaning security should be implemented from the start.

4. Achieve consensus for interoperability incentives for IoT security – try to make IoT devices that work together without any issues, everything from IoT device, platforms to frameworks.
5. Foster economic and administrative incentives for IoT security – try not to rush out new products without any security features. A reason for this is also the lack of consumer security knowledge.
6. Establish secure IoT product/service lifecycle management – have clear goals and processes during all the phases (design, development, testing, production, deployment, maintenance, end-of-support, and end-of-life) of an IoT device or services. Especially during the end-of-life when it is being decommissioned should be communicated clearly to customers.
7. Clarify liability among IoT stakeholders – the question of where liability may fall lies between the different stakeholders of the IoT environment, so developers, manufacturers, providers, vendors, aftermarket support operators and third-party providers should be clearly addressed.

3.5 Microsoft's IoT recommendations

In April of 2019, researchers from Microsoft Threat Intelligence Center (MSTIC) found that an unknown attacker was trying to compromise common and popular IoT devices, in this case a Voice over Internet Protocol phone (VoIP), an office printer and a video decoder across multiple customer locations (MSTIC, 2019).

In two out of the three cases, default password had been left unchanged, and in the third and last case the device had not been updated with the latest security updates. These devices then became the entrance points for the attacker after which they managed to establish presence and continue looking for further access. After this, according to MSTIC, the actor simply scanned for more vulnerable devices and move across to them in order to find higher-privileged accounts. While the attacker was moving on to other devices, they dropped a shell script to establish further persistence on the network. MSTIC also found that the IoT devices and the other devices where communicating with an external command and control, also known as C2, server (MSTIC, 2019).

MSTIC posted part of the script they found on the devices, which can be seen in Figure 10.

```
—contents of [IOT Device] file--

#!/bin/sh
export [IOT Device] ="-qws -display :1 -nomouse"
echo 1|tee /tmp/.c;sh -c '(until (sh -c "openssl s_client -quiet -host
167.114.153.55 -port 443 |while : ; do sh && break; done| openssl s_client -
quiet -host 167.114.153.55 -port 443"); do (sleep 10 && cn=$((`cat
/tmp/.c`+1)) && echo $cn|tee /tmp.c && if [ $cn -ge 30 ]; then (rm
/tmp/.c;pkill -f 'openssl'); fi);done)&' &

--end contents of file--
```

Figure 10. Script used to maintain access to network (MSTIC, 2019)

As result of these findings Microsoft and MSTIC released their own set of recommendations for securing enterprise IoT devices. Microsoft recommends the following steps in order to better secure and manage IoT devices (MSTIC, 2019):

1. Require approval and catalogue any IoT device in the corporate environment
2. Develop separate security policies for IoT devices
3. Avoid exposing IoT devices directly towards Internet or create custom access control
4. Use a separate network for IoT devices
5. Conduct routine configurations/patch audits against the IoT devices in use
6. Define policies for isolation of IoT devices, preservation of data, maintain logs of traffic and capture devices images for forensic investigation
7. Include IoT device configuration weakness or IoT-based scenarios as apart of Red Team testing
8. Monitor IoT device activity for abnormal behaviour
9. Audit credentials that have access to the IoT devices
10. Centralize asset management if feasible
11. If the IoT devices are deployed or managed by a third party, then include explicit term in your contract detailing security practices to be followed and audits the report their status.

12. Where possible, define SLA (Security Level Agreement) terms on IoT devices that mutually acceptable windows for investigative response and forensic analysis to any compromised products.

3.6 Tom Gaffney's from F-Secure IoT Recommendations

Tom Gaffney from F-Secures presales team visited F-Secures cybersecurity podcast called Cyber Security Sauna in episode 27 – The Connected Home Meets the IoT Tire Fire. During the podcast, Gaffney and the host Janne Kauhanen discusses the pros and cons regarding smart homes and other IoT devices. Gaffney started off by quoting his colleague Mikko Hyppönen and saying everything that is smart, is vulnerable (Hyppönen, 2016). So almost three years later and nothing has really changed according to Gaffney. He continued saying that the main reason is that the barrier to making these devices is lower than ever before and basically anyone can make an IoT device today. This usually comes from the fact that there are manufacturers that make good, decent devices that are well made but might come in a bit more expensive. As soon as these devices hit the market someone will start working on their own cheaper version of a similar device that is not as well made as the original (Gaffney, 2019).

Gaffney and Kauhanen continued discussing about a study that the F-Secure lab released at the end 2018. In the report F-Secure found that one third of the IoT vulnerabilities are open ports and another third of the vulnerabilities are default passwords, which means that some are hard coded and cannot be changed or have no password at all or are never changed from the default password the IoT device arrived with (Gaffney, 2019).

Another point they discussed was about how hackers are not necessary targeting any device specifically unless you are a high net target like a business or maybe a celebrity. That still does not stop attackers from looking for any weaknesses on the Internet and try to exploit them for their own gain. In some cases, the devices have been a part of a botnet, Mirai for instance, and in other cases bitcoin miners have been installed on the devices (Gaffney, 2019).

Gaffney also mentioned the issue with the responsibility the providers have and the power they have over the IoT devices and the of users too. Gaffney brings up the issue with Sonos where they updated their “privacy policy” and if users did not accept it the device may cease to function (Gaffney, 2019).

Kauhanen asks, how do we as a society make sure these companies are living up to their responsibilities, to which Gaffney responds that lots of governments do not wish to regulate. However, the government in United Kingdom has released the Code of Practice for Consumer IoT Security which is meant to help manufacturers create good and secure IoT devices (Gaffney, 2019). Gaffney continues by saying that there is a need for something similar to General Data Protection Regulation in the IoT world. He also mentions that there are some local laws in states like California and Oregon, but these are only local laws and does not apply to companies outside, like Alibaba for instance. Hence, there is a need for a greater framework rather than just local ones (Gaffney, 2019).

Gaffney and Kauhanen also bring up the home assistants like Google home and Alexa that were caught listening in on their users in the summer of 2019. These two assistants are connected to the cloud and ship all the data to the cloud, similar to many other IoT devices. However, Gaffney mentions that there is a new device in development that does all the voice algorithms locally and goes on and asks why other devices don’t do that too. There is a cloud connection to update the algorithms according to Gaffney but that is separate from the data which improves the privacy compared to other devices sending the data to the cloud.

Gaffney shared 6 tips on how to make IoT devices connected to the Internet more secure (Gaffney, 2019):

1. Make sure the device can be updated
2. Force a default password change
3. Have a patch mechanism
4. Run a bug bounty program
5. Map the device’s attack surface
6. Collect only the data needed

Some other tips shared by Gaffney for the IoT consumers was to download the app first (if the device has one) and read the reviews about the device to get a better understanding of how other users value the device. If the device is still interesting and one does end up buying it, then change the password right immediately when you are setting up the device. That removes one third of the vulnerabilities according to Gaffney. The third advice is to set up a separate IoT network, if one has the knowledge for it. That way the device is isolated and potential issues and risks related to it.

3.7 United Kingdom's IoT Guidelines

As mentioned earlier, the UK government has created their own set of best practices. It is mainly intended for the smart homes rather than ICS or the health industry. These recommendations can be found in the document The Code of Practices for Consumer IoT Security from the Department for Digital, Cultures, Media and Sport. The code was published in March of 2018 with the help of National Cyber Security Centre (NCSC).

The goal of this summary is to make sure that as people entrust an increasing amount of personal data to online devices and services that the manufacturer should make sure that these devices have the same level of security as the physical security of the homes. These recommendations are set to help all parties involved in the development, manufacturing and retail of these consumer devices. These guidelines are what is widely considered good practice in IoT security (NCSC, 2018). They are outcome-focused rather than prescriptive which will provide organizations some flexibility to innovate and implement security solutions appropriate for their products (NCSC, 2018).

The Code of Practices claims that it is not some silver bullet which will solve all the problems within the IoT security world but is intended to shift the mindset to a more secure development mindset. These kinds of products and services should be designed with security in mind from the start and not just added on later as some sort of feature. It also wants organizations to every now and then assess

the risks in order to maintain a good level of security on the products and services they offer (NCSC, 2018).

The Code of Practices also brings up the supply chain into their recommendations. The supply chains of IoT products and be complex and international and often involves multiple component and manufacturers and service providers (NCSC, 2018). The aim to maintain a positive and secure change throughout the entire supply chain (NCSC, 2018).

3.7.1 The Code of Practices

The first three are meant to be prioritized as these on their own will greatly improve IoT security, hence they are a bit differently coloured in Figure 11 compare to the other numbers (NCSC, 2018).

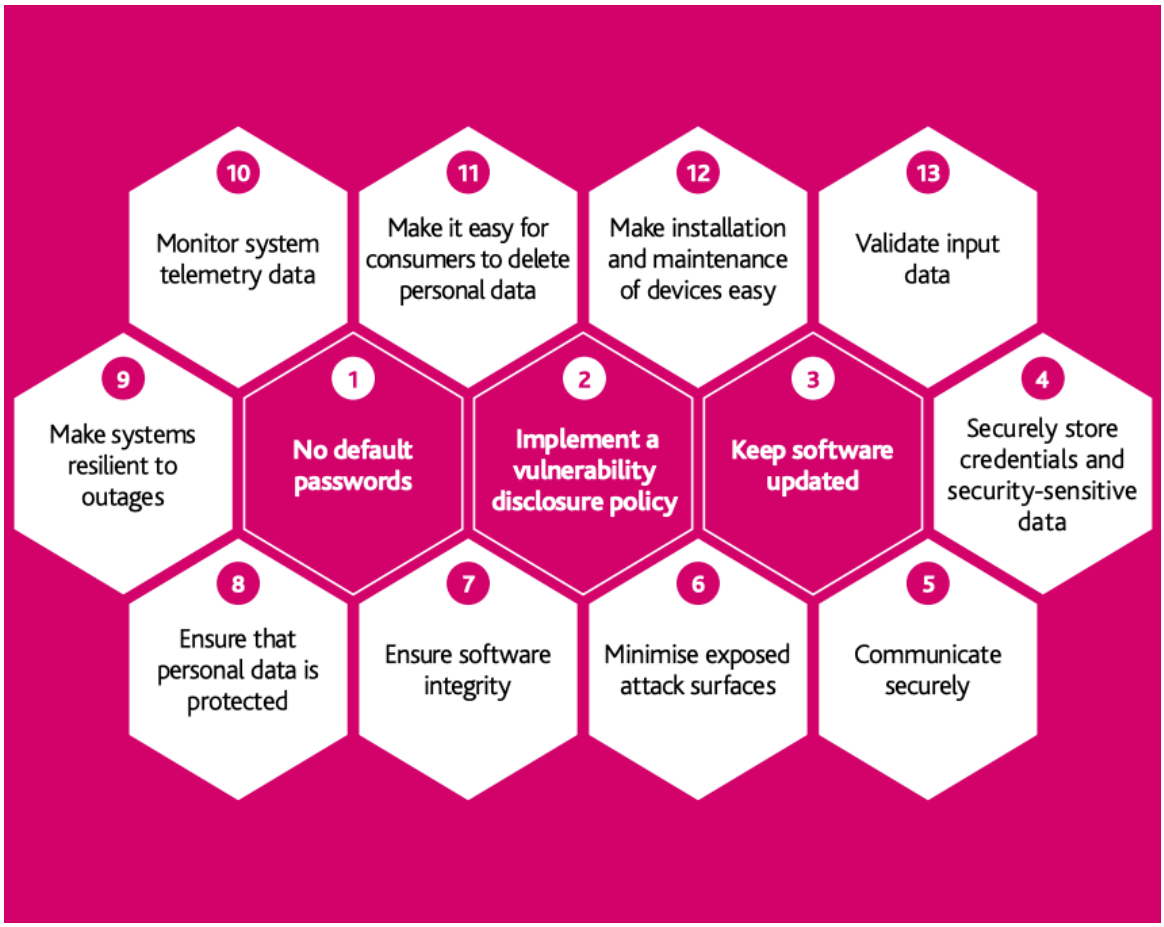

Figure 11. 13 top IoT issues

1. No default passwords – all IoT devices passwords should be unique and not resettable to a universal default value.
2. Implement a vulnerability disclosure policy – provide a public point of contact as a part of vulnerability disclosure.
3. Keep software updated – have an update option and publish patches that fix vulnerabilities.
4. Securely store credentials and security-sensitive data – any credentials shall be stored securely on the device or service. Hardcoded credentials are not acceptable.
5. Communicate securely – security-sensitive data including remote management be should be encrypted while in transit. All keys should be managed securely.
6. Minimize exposed attack surfaces – devices should be operating with the principle of least privilege, unused ports should be closed, hardware should not be exposed, services should not be available if not used.
7. Ensure software integrity – if an authorized change is detected then the device should inform the user and should not connect to wider networks than needed for alerts.
8. Ensure that personal data is protected – if devices process personal data, they should follow data protections laws such as General Data Protection Regulation.
9. Make systems resilient to outages – devices should be able to function without network and recover without any issues in case of a power outages.
10. Monitor system telemetry data – have an ability to monitor for security anomalies.
11. Make it easy for consumers to delete personal data – consumer should be given clear and easy instructions on how to delete personal data.
12. Make installations and maintenance of devices easy – minimal steps and should follow security best practice on usability.
13. Validate data input – all data should be validated to make sure it does not contain executable code or values beyond limits.

3.8 OWASP

Open Web Application Security Project (OWASP) foundation was created in early December of 2001. It was established to improve security through its community. The OWASP project is an open community dedicated to enabling organizations to conceive, develop, acquire, operate and maintain application that can be trusted (OWASP, 2020). They have created tools, documents, forums and chapters that are free to use by anyone that is interested in improving security in different fields like IoT. They have also created a detailed attack surface map for the IoT environment.

3.8.1 OWASP IoT attack surface

As mentioned earlier OWASP, has created a detailed attack surface map for the IoT environment. This map is a part of the OWASP Internet of Things Project which is led by Daniel Miessler and Craig Smith among others. The idea with the map is to help manufactures, developers, security researchers and those looking to deploy IoT device in their organization understand all the different risks and potential vulnerabilities within an IoT environment. (OWASP, 2019). Information regarding how the map was constructed was not mentioned. The map can be seen in Figure 12.

Attack Surface	Vulnerability
Ecosystem (general)	• Interoperability standards • Data governance • System wide failure • Individual stakeholder risks • Implicit trust between components • Enrollment security • Decommissioning system • Lost access procedures

Device Memory	• Sensitive data
	  • Cleartext usernames
	  • Cleartext passwords
	  • Third-party credentials
	  • Encryption keys

Device Physical Interfaces	• Firmware extraction
	• User CLI
	• Admin CLI
	• Privilege escalation
	• Reset to insecure state
	• Removal of storage media
	• Tamper resistance
	• Debug port
	  • UART (Serial)
	  • JTAG / SWD
	• Device ID/Serial number exposure

Device Web Interface	• Standard set of web application vulnerabilities defined by OWASP

	• Credential management vulnerabilities:
	  • Username enumeration
	  • Weak passwords
	  • Account lockout
	  • Known default credentials
	  • Insecure password recovery mechanism

Device Firmware	• Sensitive data exposure
	  • Backdoor accounts
	  • Hardcoded credentials
	  • Encryption keys
	  • Encryption (Symmetric, Asymmetric)
	  • Sensitive information
	  • Sensitive URL disclosure
	• Firmware version display and/or last update date
	• Vulnerable services (web, ssh, tftp, etc.)
	  • Verify for old sw versions and possible attacks (Heartbleed, Shellshock, old PHP versions etc)
	• Security related function API exposure
	• Firmware downgrade possibility

Device Network Services	• Information disclosure
	• User CLI
	• Administrative CLI
	• Injection
	• Denial of Service
	• Unencrypted Services
	• Poorly implemented encryption
	• Test/Development Services
	• Buffer Overflow
	• UPnP
	• Vulnerable UDP Services
	• DoS
	• Device Firmware OTA update block
	• Firmware loaded over insecure channel (no TLS)
	• Replay attack
	• Lack of payload verification
	• Lack of message integrity check
	• Credential management vulnerabilities:
	  • Username enumeration
	  • Weak passwords
	  • Account lockout
	  • Known default credentials
	  • Insecure password recovery mechanism

Administrative Interface	• Standard set of web application vulnerabilities defined by OWASP
	• Credential management vulnerabilities:
	  • Username enumeration
	  • Weak passwords
	  • Account lockout
	  • Known default credentials

	• Insecure password recovery mechanism • Security/encryption options • Logging options • Two-factor authentication • Check for insecure direct object references • Inability to wipe device
Local Data Storage	• Unencrypted data • Data encrypted with discovered keys • Lack of data integrity checks • Use of static same enc/dec key

Cloud Web Interface	• Standard set of web application vulnerabilities defined by OWASP
	• Credential management vulnerabilities:
	  • Username enumeration
	  • Weak passwords
	  • Account lockout
	  • Known default credentials
	  • Insecure password recovery mechanism
	• Transport encryption
	• Two-factor authentication

Third-party Backend APIs	• Unencrypted PII sent • Encrypted PII sent • Device information leaked • Location leaked
Update Mechanism	• Update sent without encryption • Updates not signed • Update location writable • Update verification • Update authentication • Malicious update • Missing update mechanism • No manual update mechanism
Mobile Application	• Implicitly trusted by device or cloud • Username enumeration • Account lockout • Known default credentials • Weak passwords • Insecure data storage • Transport encryption • Insecure password recovery mechanism • Two-factor authentication
Vendor Backend APIs	• Inherent trust of cloud or mobile application • Weak authentication • Weak access controls • Injection attacks • Hidden services
Ecosystem Communication	• Health checks • Heartbeats

	• Ecosystem commands • Deprovisioning • Pushing updates
Network Traffic	• LAN • LAN to Internet • Short range • Non-standard • Wireless (WiFi, Z-wave, XBee, Zigbee, Bluetooth, LoRA) • Protocol fuzzing
Authentication/Authorization	• Authentication/Authorization related values (session key, token, cookie, etc.) disclosure • Reusing of session key, token, etc. • Device to device authentication • Device to mobile Application authentication • Device to cloud system authentication • Mobile application to cloud system authentication • Web application to cloud system authentication • Lack of dynamic authentication
Privacy	• User data disclosure • User/device location disclosure • Differential privacy
Hardware (Sensors)	• Sensing Environment Manipulation • Tampering (Physical) • Damage (Physical)

Figure 12. OWASP IoT attack surface map (Draft) (OWASP, 2019)

As can be seen from the Figure 12 the attack surface can potentially be massive in an IoT environment. It is not only the physical device that needs security but the whole environment, network traffic, web interface, cloud and so on. This list contains a majority of potential attack surfaces that can be found in the IoT world but that does not mean that every single IoT device faces these potential risks. A good example would be in case an IoT device is not in any way connected to the cloud it will not have the cloud as a potential attack surface.

Some other information that can be read is that all the previously mentioned issues from the other cases can be found on this list. One can also assume that the issues in Figure 12 are not ranked by severity, since then the default password issues would clearly be at the top of the list. With help of this map manufacturers can get additional information about potential attack surfaces they did not think of and either have them secured or removed if not needed.

3.8.2 OWASP Top 10 issues

OWASP has also created a Top 10 issues seen in IoT environments from 2014 and 2018. Their idea behind this list is represent the top issues seen when building, deploying and managing IoT Systems (OWASP, 2019). They also opted for simplicity by creating one list instead of having a separate list for developers and one for enterprises and one for consumers. The two lists can be seen in Figure 13.

	2014	2018
1.	Insecure Web Interface	Weak, Guessable or Hardcoded Passwords
2.	Insufficient Authentication	Insecure Network Services
3.	Insecure Network Services	Insecure Ecosystem Interface
4.	Lack of Transport Encryption	Lack of Secure Update Mechanism
5.	Privacy Concerns	Use of Insecure or Outdated Components
6.	Insecure Cloud Interface	Insufficient Privacy Protection
7.	Insecure Mobile Interface	Insecure Data Transfer and Storage
8.	Insufficient Security Configuration	Lack of Device Management
9.	Insecure Software/Firmware	Insufficient Security Configuration
10.	Poor Physical Security	Lack of Physical Hardening

Figure 13. OWASP Top Ten Mapping (OWASP, 2019)

4 RESULTS OF THE STUDY

Based on the different cases there are common areas that needs security improvements and that there a no common guidelines. Every case is referring to its own guidelines and issues or other areas that needs security improvements. In

some cases, the cases provide solutions to the issues. However, all the cases seem to point the same issues.

Some of the areas are more critical than others due to the high amount detected and some due to the impact the issue might have if they are exploited and finally in some cases it is both reasons. An example of that would be default passwords, which is seen quite often and can easily be exploited by a simple google search of the product in question.

There is no general guidance or certificates that the IoT manufacturers could use in order prompt a healthy security environment or approach. This is seen as all the different cases have their own recommendations instead of referring to a NIST, ENISA or ISO approved method, guide or certificate.

In order to avoid these kinds of issues this thesis will put together security guidelines and recommendations on a general level so that it can be applied to any IoT devices. The guidelines and recommendations can be applied to any device and then improved upon in case seen fit or needed, as different areas might have different demands. For instance, IoT devices from the health industry might need comply to Health Insurance Portability and Accountability Act (HIPAA) and IoT devices that handle credit cards information needs to be complaint with the Payment Card Industry Data Security Standard (PCI DSS).

4.1 The mind set

First and foremost, security needs to be a part of the design, from the beginning. When devices are being planned, the devices should be planned with security in mind. Security should not be added as a late extra feature because it is the right thing to do. Also, IoT security does not mean physical security only (Miessler, 2015).

The companies could themselves be a bit more proactive in raising awareness and maybe even provide a bit of training on how to secure IoT their devices. By doing so it will improve the IoT community as a whole and at the same time give

a good picture of the company handle and treat security. It could be something as simple as a YouTube video installation guide.

IoT manufacturers also need to remember that even though they put a lot of thought into planning and developing security for their devices, part of security is keeping in mind that the supply chain can also be affected. In other words, the hardware or third-party software used in the IoT devices needs to be from an approved vendor that also takes security seriously. This too should be reviewed occasionally by the IoT manufacturers. Buying the cheapest parts or/and software is not always the best solution in order to keep and provide a good and manageable security. It might lower the cost of the device, but it will most likely not improve the security of it.

IoT manufacturers also need to remember that user friendliness and security does not always go hand in hand but in the long-term security will win you over more customers. Having easily configurable devices versus plug and play can affect sales as some users might not want to deal with any hassle of being forced to configure the device. However, having security configuration requirements is required in order to improve security.

Making sure protocols and features are not turned on by default is another great way of improving security. Limiting the attack surface in any way possible is always a great option in order to improve the security. An example of this is universal plug and play (UPnP) protocol is recommended to not having turned on as it is an easily exploitable protocol. This was first reported by Daniel Garcia in 2006 at Defcon19 (Akamai, 2018). In the case of the UPnP protocol the IoT owner might not be the victim of the attack but is still used in order to commit a criminal act (Akamai, 2018).

4.1.1 The model

By following the NIST CSF model, a cybersecurity framework, the most urgent issues have been identified. The NIST CSF model, as seen in the Figure 14, contains and starts with identify, protect, detect, respond, recover and then it

starts all over again from identify (NIST, 2018). One needs to remember the security is something that is always ongoing and not something static that is done once and then it is completed, hence the circle simulates perfectly security.

Figure 14. NIST CSF v1.1 (NIST, April 2018)

4.2 IoT issues compiled

The issues identified have divided into four phases. Planning and Creation, Installation, In Use and End of Life. These phases are meant to make it a bit clear when different an issue can be spotted and potentially fixed. Some issues might still appear in more than one of the phases.

The issues listed are not arranged in any particular order, but the most critical issues seen will be in the be listed with suggested solutions, evaluation techniques and a level of impact (low, medium, high and critical).

4.2.1 Planning and creation phase

Phase	Number	Issue	Solution
1. Planning and Creation	1	No security mindset	The device should be planned and built with security in mind.
	2	Security is only added at the end of the creation phase	The device should be planned and built with security in mind from the beginning.
	3	Devices are planned with only physical security	Security should not be planned only for the physical device but the whole system
	4	Unnecessary ports left open	Close unused ports and features
	5	A security evaluation is not done to the final product	Any changes to a device would require a security evaluation to make sure it is still safe and secure
	6	Attack surface is not evaluated	Attack surfaces needs to be evaluated
	7	User data disclosure and sharing	Evaluate if sharing the data is really needed and if deemed needed the make sure to

			inform the users and potentially have an opt-out option.

Figure 15. Creation phase table

4.2.2 Installation phase

Phase	Number	Issue	Solution
2. Installation	1	Not easy to install (software)	Make sure the devices are easy to install and provide an installation guide
	2	Hardcoded passwords	Do not use hardcoded passwords and create a “create user phase” with password restrictions like 8 characters long etc.
	3	Defaults password	Do not use default passwords like admin/admin. Ask the user to create a new user phase with password restrictions like 8 characters long etc.
	4	Information gathering	Do not ask for information, which is not needed, i.e. Smart home devices to do not need social security information.

	5	User training	A simple YouTube video would greatly improve user's knowledge of how the device works.
	6	Data storage	Is data storage needed? If it is needed can it be stored locally instead of the cloud? If cloud storage is needed make sure it is secured. If local is enough, make sure the local device is secure and guide users through it they need to do something.
	7	Internet access	Does every device need Internet access? A hub/controller would be enough for updates etc. to avoid having all the devices connected to the Internet.
	8	Not easy install (physically)	Provide all needed parts to make the

			physical installation easy and a guide

Figure 16. Installation phase table

4.2.3 In Use phase

Phase	Number	Issue	Solution
3. In Use	1	No updates option available	Make sure updates are available and have a process for updates
	2	No management option or feature	A hub with a GUI (graphical user interface) would be able control and management several devices at once
	3	No interoperability	Do not lock down the devices so they do not work with other environments
	4	No wipe or reset ability	Make sure that a data wipe or reset feature is available
	5	All or many features are turned on by default	Do not turn on all features by default. Allow the user during installation phase to turn those which they want and then have the option to turn on more later
	6	Not resilient to outage	If the device is turned off, for any reason at all, make sure they are not reset because of that

7	No logs available	Allow the device to store and show logs of what's going on with the device
8	Hard to maintain	The devices should be easy to update, change settings. Again, a hub with GUI would be perfect
9	Unnecessary ports open	Close unused ports
10	Little to no security awareness	Trying to stay active with information about security and other updates
11	Bugs cannot be reported easily	Join a bug bounty program like hackerone, bugcrowd or EU FOSSA
12	A security evaluation is not done to the product	Security is not something static and should be evaluated constantly
13	No hardware support	*This might be a risk the customer might have to accept, depending on the device. Some have replacement hardware parts while others don't. Asking to have everything part*

			available for replacement is not always possible.
	14	Device locations disclosure	An option that could be turned off and on by the user if needed
	15	Firmware updates missing	Make firmware updates available and make sure they are signed and secure
	16	Two-factor authentication is not an option	Have an option to enable two-factor authentications
	17	Health check ins and information missing (management)	Provide an easy to use GUI which informs the user about missing updates, devices offline etc.

Figure 17. In Use phase table

4.2.4 End of Life phase

Phase	Number	Issue	Solution
4. End of Life	1	Not easy to decommission	Decommission should be made easy with a built-in option to wipe the device
	2	Not clear End of Life information	How long a device is in use may vary a lot depending on the area. This information needs to be communicated clearly.
	3	No wipe data or overwrite data option	A hub would be able to control and erase all data and settings from the devices and then lastly from the hub itself.

Figure 18. End of Life phase table

4.3 Evaluation of the IoT systems

Now that the most common issues have been identified and solutions to the issues have also been identified, how does a manufacture or an owner of an IoT devices know if one of their devices are affected with any of these mentioned issues?

Note that some of the issues spotted cannot be evaluated. As an example, “Security is only added as a late feature or at the end of the creation phase”, there is no way to evaluate this as it is not cyber security vulnerability that can be exploited. For cases like this the note “not a vulnerability” will be mentioned as there is not evaluate.

4.3.1 Issues from Planning phase

Number	Issue	Evaluation
1	No security mindset	Not a vulnerability that can be evaluated but it is still a risk
2	Security is only added as a late feature or at the end of the creation phase	Not a vulnerability but a risk as it will be easier to add security gradually rather than “all at once” in the end.
3	Devices only have physical security	This will be quickly noticed just by using a vulnerability scanner like Nessus or a port scanner like NMAP and scanning the device. They will most likely show up unused ports and other vulnerabilities.
4	Unnecessary ports left open	NMAP scan of the device(s) to see what kind of ports are open
5	A security evaluation is not done to the final product	Not a vulnerability but assuming an evaluation has been done once, it is still needed again after a change since that change might have affected the device somehow and to confirm the change fixed the issue.
6	Attack surface is not evaluated	Not a vulnerability but after every change done to the device an evaluation would be a good thing to perform.
7	User data disclosure and sharing	This issue is usually done on the backend. Sharing collected user information or device usage with 3rd party partners meaning an evaluation cannot detect this issue. Assuming however, that the manufacturers follows good conduct they will inform about this in their policies and user agreements, who has access to what data and why also.

Figure 19. Creation phase issues

4.3.2 Issues from Installation phase

Number	Issue	Evaluation
1	Not easy to install (software)	Not a vulnerability but a risk as the users could leave the device open for attacks as it is too hard to secure. Also, what needs to be considered is that what one person considers easy might not be easy for the next person.
2	Hardcoded passwords	Usually found in the manual as Login: Admin and Password: Admin or something similar and if it is not found there a quick google search should be able to provide it, that is if the device is facing this issue.
3	Defaults password	Usually found in the manual as Login: Admin and Password: Admin or something similar and if it is not found there a quick google search should be able to provide it, that is if the device is facing this issue.
4	Information gathering	While setting up the device or account this will be encountered. What information is needed or not needed but still asked for during setup. A smart lamp should not need a personal security number while a medical IoT device might need it.
5	User training	Confirm whether the manufacture provides training/user videos for the device in their community
6	Data storage	Assuming the manufacturer follows a good consumer conduct they inform where the data is stored, and it should be available in their user policy or agreement. Is sent to the cloud or is it stored locally on the device? If the data is sent to the cloud, there really is not much a user can do. If the is stored locally on the device, then hopefully the device has been equipped with

		enough security features to allow the users to secure them.
7	Internet access	Scanning your IP (which can be found with the help of site like https://whatismyipaddress.com/) with tools like Shodan (https://www.shodan.io) and Thingful (https://www.thingful.net/) will show what devices are exposed to the Internet and how.
8	Not easy install (physically)	Not a vulnerability but a risk as the users could leave the device open for physical tempering as it is too hard to secure. Also, what needs to be considered is that what one person considers easy might not be easy for the next person.

Figure 20. Installation phase issues

4.3.3 Issues from Use phase

Number	Issue	Evaluation
1	No update option available	Done from the device or the management application. Confirm whether there is an option to update/check for updates available. If available, it could be worth confirming when the last update was released too to make sure this feature is in use.
2	No management option or feature	Application or hub to manage several devices at once. At least from the same manufacture but even better would be to manage other devices too of similar type, like smart lamps of different provider can be added to one hub to control and update.
3	No interoperability	Application or hub to manage several devices at once. Manage other devices of similar type, like smart lamps of different providers can be added to one hub to control and update.
4	No wipe or reset ability	Easiest way to confirm whether the device is resettable is to check the manual or the management application for a reset or wipe option and test it to make sure it works.
5	All or many features are turned on by default	Easiest way to confirm whether the device has everything turned on is to check the management application and through it confirm which features are turned on. Are all? If it is possible to turn off undesired features that is good, assuming the user can control it. However, better would be to turn on needed features rather than having all turned on by default. An example would be location sharing. Is this a feature that the user can control? And if so, is it turned on by default or not?

6	Not resilient to outage	After the device has been configured as desired, unplug the power cable and plug it in again to confirm whether the settings are still in place and the device is working in the same way as it did before.
7	No logs available	Best way of confirming whether the device have logging capability is to confirm with the manufacturer of the device, either by googling or reading through the manual provided with the device.
8	Hard to maintain	Does the device have an application or hub to manage several devices at once?
9	Unnecessary ports open	NMAP scan of the device or is it setting(s) that can be turned off. For example, SSH from a WebGUI.
10	Little to no security awareness	Does the manufacturer have a community forum, blog or similar which they actively use to communicate with their community about issues and upcoming change and features? To confirm this the easiest way is to go their website or management application to confirm if the manufacturers has this option.
11	Bugs cannot be reported easily	Confirm if the manufacturer has joined a bug bounty community like hackerone (https://hackerone.com/) or bug crowd (https://www.bugcrowd.com/) as this shows that they have good security hygiene and also allow users to help with securing the environment.
12	A security evaluation is not done to the product	Assuming an evaluation has been done, something might still have changed afterwards, and the change has opened the device for a vulnerability.
13	No hardware support	Not a vulnerability but a risk – if the device breaks it breaks. However, confirm with the manufacturer what kind of support they have for the device.

14	Device locations disclosure	Is this a feature the user can control? And if so, can it be turned off in settings or somewhere else.
15	Firmware updates missing	Done from the device or the management application. Confirm whether there is an option to update/check for updates available. If available, it could be worth confirming when the last update was released too to make sure this feature is in use.
16	Two-factor authentication is not an option	Two-factor or multifactor authentication is an option that would be in the management interface. if it is an option, if can maybe be found under settings and configured or maybe configured during first setup.
17	Health check ins and information missing (management)	If the device has a management feature, within that feature having the option to view what all the devices statues are (online or offline etc.) and whether a new patch is available etc.

Figure 21. In Use phase issues

4.3.4 Issues from End of Life phase

Number	Issue	Evaluation
1	Not easy to decommission	Is decommission even an option? Easiest way to confirm whether the device is resettable is to check the manual or the management application for a reset or wipe option. All data and configurations should hopefully be easily removed if the option is available. Otherwise physically destroying the device is an option but depending on the device it might be easier said than done.
2	Not clear End of Life information	Not a vulnerability but a huge security risk (depending on the device) as consumers will need to know when a device is going to stop receiving support. This can only be evaluated in case the manufacturer has created devices before and check how well they communicated the end of life of them if they have reached EOL that is.
3	No wipe data or overwrite data option	Easiest way to confirm whether the device is resettable is to check the manual or the management application for a reset or wipe option. All data and configurations should hopefully be easily removed if the option is available.

Figure 22. End of Life phase issues

4.4 Categorizing the issues

In order to get a better overview of how severe the top issues can be, this thesis will categorize them from low, medium, high and critical in order to demonstrate the impact these issues have if found on a device. Low will not mean it should be avoided or can be postponed. As pointed out in the cases these issues are known recurring issues. It is only low compared to those issues that are marked high or critical. Colours are added to make easier identify the difference in the levels. Numbers do not represent any ranking of the issues. They will be kept to easier to do a follow from the previous sections in this thesis.

An estimated cost in case an issue is exploited will be hard to estimate as the variation of the cost depends on the environment of the device. A compromised printer at home might not affect the owner at all while a robotic arm at a factory could put people's life's in danger or cause physical damages to property in-case it is tampered with.

The level-summary will be done on a general level, in other words, an impact might be low on some IoT devices it could be critical on others, depending on the environment, then the issue will be considered critical. An example of how an issue could affect different devices differently in different situations is log management. It might not be an issue for smart home users if there is not log management features while it can be crucial for the ICT industry in order to do follow ups. Log management availability might not break the system, but it is easier to follow ups on issues and manage devices if logs are available.

4.4.1 Categorization of issues in Planning phase

Phase	Number	Issue	Level-Summary	Reason
1. Planning and Creation	1	No security mindset	High	In theory, it doesn't break the device and can be improved upon
	2	Security is only added as a late or at the end of the creation phase	High	One can miss or forget something in case it's added later instead of right immediately
	3	Devices only have physical security	Critical	While physical security is good, the majority of the issues seen are software related
	4	Unnecessary ports left open	Critical	Exposes the devices
	5	A security evaluation is not done to the final product	Critical	Vulnerabilities will be unknown
	6	Attack surface is not evaluated	High	One might miss something unless this is done
	7	User data disclosure and sharing	Medium	Privacy is a right not a feature. Users should be deciding if they want to share information or not

Figure 23. Categorization of issues in planning phase

4.4.2 Categorization of issues in Installation phase

Phase	Number	Issue	Level-Summary	Reason
2. Installation	1	Not easy to install (software)	Medium	This might lead to exposed ports, mistakes etc. in case it is hard to install
	2	Hardcoded passwords	Critical	Passwords you cannot change but Google, exposes the IoT environment
	3	Defaults password	Critical	Passwords you Google exposes the IoT environment
	4	Information gathering	High	Privacy is a right not a feature. Users should be deciding if they want to share information or not
	5	User training	Low	For ICT hopefully users get training while smart home users mostly likely will not
	6	Data storage	Low	Storing the data in the cloud is not an issue but

				securing can be
	7	Internet access	Medium	Not all devices need to be exposed to the Internet and should not be
	8	Not easy install (physically)	Low	Depending on the device, one could argue for a higher level but generally it is low. If expertise is needed, then hopefully the manufacturer can provide training or experts

Figure 24. Categorization of issues in installation phase

4.4.3 Categorization of issues in Use phase

Phase	Number	Issue	Level-Summary	Reason
3. In Use	1	No update option available	Critical	Vulnerabilities needs to be patched
	2	No management option or feature	Critical	Management is needed in order keep the environment safe and secure and easier to manage
	3	No interoperability	High	Forcing users into a specific brand is not good in the long run
	4	No wipe or reset ability	Critical	Users need to be able to delete the data and configurations from the devices
	5	All or many of the features are turned on by default	High	Better have them turned off and allow users to turn on what they need
	6	Not resilient to outage	Critical	Reinstallation and configuration should not be needed in case the device loses power
	7	No logs available	High	For home users this is not an issue but for businesses it is recommended
	8	Hard to maintain	High	Hard maintenance increases the risk for mistakes
	9	Unnecessary ports open	Critical	Exposes the devices

	10	Little to no security awareness	High	Unless issues are communicated the users cannot fix them.
	11	Bugs cannot be reported easily	High	If users can find issues and want to help, give them the option to help
	12	A security evaluation is not done to the product	High	One will never know what issues exist after an update unless it is checked
	13	No hardware support	*Critical*	Depending on the device is it critical. All hardware can understandably not be replaced
	14	Device locations disclosure	High	A feature that should be turned off and only turned on if users wish to share this information
	15	Firmware updates missing	*Critical*	Firmware updates are as critical as software updates
	16	Two-factor authentication is not an option	Medium	Only set as medium as it improves security, but a device can still be secure without it
	17	Health check ins and information missing (management)	Medium	Only set as medium as it improves security, but a device can still be secure without it

Figure 25. Categorization of issues in use phase

4.4.4 Categorization of issues in End of Life phase

Phase	Number	Issue	Level-Summary	Reason
4. End of Life	1	Not easy to decommission	High	Increases the chances of mistakes in case the process is hard
	2	Not clear End of Life information	High	This information needs to be clearly communicated for users to act and prepare for these kinds of changes
	3	No wipe data or overwrite data option	Critical	Users need to be able to delete the data from the devices before the device leaves their premises

Figure 26. Categorization of issues in end of life

4.4.5 Summarization of categorization

As this section demonstrates, these issues are crucial and critical to take care of. There are 13 classified as critical issues out of the 35 mentioned and 14 are classified as high since they too could have severe consequences in case they are not dealt with.

Some of them are marked “only” as low as the impact they could have would be minor, like the physical installation, while others are critical, like wiping data off the IoT devices. However, no matter of the categorization they need to be fixed in order to improve IoT security.

4.5 Evaluating an IoT device

Final thing to do in order to evaluate an IoT device is to do the evaluation itself. The evaluation can be divided into six different stages. The stages would be

Inspection, Installation, Information and monitoring, Penetration testing, Reset/Decommission the device and Reporting the findings. These stages are initially based on the conference paper Penetration testing for Internet of Things and Its Automation written by Ge Chu and Alexei Lisitsa. In their paper they have listed four stages, Information gathering, Analysis, Exploitation and Reporting but their paper is focused on penetration testing and automation (Chu and Lisitsa, 2019). As this section focuses on evaluation this thesis suggests adding these two stages to the evaluation, installation and decommission. As seen in the cases there were issues found during installation and decommission as well.

4.5.1 Inspection

First thing to do is to inspect the device in question to in order to understand what potential risks can be found physically.

- Exposed buttons
    - On/off button
    - Reset button
- Exposed ports
    - USB port(s)
    - Network port
    - Power cable
    - Other ports
- Is it possible to access the internal hardware? Was it easy?
- Are there any other things you can tamper with?

4.5.2 Installation

The next stage is about installing and setting up the device. Both physically and software installation. It would also be recommended to follow the installation instructions provided, assuming any instructions were provided. Reason for this is to follow up and see what kind of instructions are provided as knowledge of installation may vary quite a lot between consumers. Also, this will show how the manufacturer handles “setting up an account” in their IoT environment as this was one of the biggest issues in the IoT world right now. Is the manufacturer

forcing users to set up a new account? Does the manufacturer have any username and/or password restrictions or is it just possible to login with username admin and password admin and just leave it?

4.5.3 Information and monitoring

During this stage information will be gathered while monitoring the device. Tools such as NMAP and Nessus can be used during this stage to see what network ports are exposed and what known vulnerabilities can be found.

While in this stage one can and should utilize Wireshark in order to monitor the network traffic from and to the device. This way one can see what the device is communicating with and what is trying to communicate with the device. Maybe the device is sending some information to some servers it is not supposed to or just trying to send something.

Another import aspect possible to monitor with Wireshark is if the traffic is encrypted or not. Potential clear text traffic like user login and password could be captured.

During this stage one will be able to find potential vulnerabilities that can be exploited during the next stage, the penetration test.

4.5.4 Penetration test

The actual penetration testing will let the tester know what exploitations are viable and show how far one is able to advance. From a penetration test perspective, the objective is to try every weakness and vulnerability identified to in the IoT environment from the earlier stages.

Chu and Lisitsa have covered this stage well in their conference paper. Their suggestion is to break the penetration stage up into three smaller stages, the Perception Layer, the Network Layer and the Application Layer (Chu and Lisitsa, 2019).

The Perception Layer, which is also known as the physical layer, the following attacks could be tried to name a few (Chu and Lisitsa, 2019):

- Skimming, reading the information off the IoT device.
- Eavesdropping, listen in on the device while it talks to other devices.
- Spoofing, creating a fake node.
- Access control attack, using a tool like IoTSeeker to break into devices.
- Killing, stealing and destroying the node

The Network Layer, which handles the information transmission between the other perception layer and application layer. During this stage the following attacks could be tested (Chu and Lisitsa, 2019):

- Signal hijacking, taking control of the Wi-Fi signal for instance.
- Signal replay, sending the same information again to a device.
- Signal fake: generate fake Information
- Network traffic sniffer: listen in on the traffic

The Application Layer, it is about the applications. This stage includes web application attack, software buffer overflow and password attacks (Chu and Lisitsa, 2019).

4.5.5 Reset/Decommission the device

The second last stage in evaluation is to reset and decommission the device. Again, issues reported in the cases was that it was not easy or sometimes not possible to reset or decommission a device. As a last result a consumer can physically destroy an IoT device once they wish to decommission it but that should not be the requirement.

If the device has a decommission option, does that option also contain some sort of data overwrite? So that it just doesn’t delete the data but also overwrites the data. Depending on the device it might contain personal identifiable information which should not only be deleted but overwritten.

4.5.6 Reporting the findings

Last and final stage is the reporting the findings from the previous stages. Potential vulnerabilities, first and foremost should be reported. As these are the greatest risks. Which exploitations were successful and was it possible to get root access are some of the examples that needs to be reported on as well. Everything from unintended access to unintended operation to unintended information access should be reported.

Any issues found should be reported so the manufacturer is able to improve the security on the device. If possible recommended solutions to the problems should also be a part of the report.

5 DISCUSSION

The suggested guidelines and recommendations will eliminate over 2/3 of all the major and common issues seen today in the IoT world. As mentioned by Gaffney from F-Secure, 1/3 of the issues they saw were related to default passwords not being changed (Gaffney, 2019). Another major issue seen today is open ports towards the Internet such as TCP Telnet, SMB and SSH and UDP UPnP (F-Secure, 2019).

These guidelines and recommendations will also ensure that the users will receive IoT devices that should be easy to install, easy to maintain and easy to decommission. This means users will not necessarily have to be computer experts or security experts in order to securely setup and maintain the IoT devices and environments. There should be some requirements during the installation phase, such as a user setup process which guides the user through the installation process with a set of minimal requirements. IoT devices should not be plug and play. That is just bad design even thought it might seem user-friendly.

One thing that maybe Internet modem providers and manufacturers for home users could do to contribute to IoT security, is to setup an IoT network or virtual

LAN (local area network) on the modem. Keeping in mind it should not be enabled by default, but still easy for the users to turn on if needed. This way users can easily sperate IoT devices on a separate virtual LAN. This is measurement should be done by everybody. Even FBI recommended this solution by saying that the fridge and laptop should not be on the same network (Steele, 2019).

Speaking of home users, these guidelines and recommendations have put a lot of focus on how manufacturers should improve security around IoT devices and environments. However, home users also need to step up their efforts in making sure the Internet is a better place. One way of doing this is not buying cheap knock off devices. As Gaffney mentioned, as soon as some IoT devices hit the market someone else will starts working on their own cheaper version of a similar devices that is not necessarily as well made as the original (Gaffney, 2019).

Another aspect that could also improve the IoT community is if either NIST or/and ENISA could adapt a framework that they approve and maintain. Even an ISO certification would be a nice feature which would be needed to be renewed every 3 – 5 years to stay relevant.

One need to remember that security is something that needs to be re-evaluated all that time. It is not something static that never changes. What is secure today might be unsecure tomorrow due to an unknown bug or vulnerability. So, no matter which framework or guidelines are followed security should be checked with regular intervals in order to maintain a secure environment.

5.1 Brickerbot

Because of all the issues see in the IoT world some users have started to take matters into their own hands in order to make the Internet a more secure place. At least according to themselves. This can be seen in the examples of the Brickerbot and the Wifatch worm, which were both bot networks that scan Internet for vulnerable Internet facing IoT devices. What happens when they identified a vulnerable device then depended on which bot found it.

The brickerbot, which was created by “the Janitor” according to Ran Levi from the podcast Malicious Life, bricks the IoT device. In other words, it destroys the IoT device (Levi, 2017). The brickerbot would destroy all the files on the device’s memory. This meant that no factory reset would fix the device either as there was nothing left to reset from (Levi, 2017). The brickerbot has since been deactivated by the creator but not before destroying over 10 million IoT devices, according to the Janitor, in the “Internet Chemotherapy” project (Cimpanu, 2017).

The Wifatch bot on the other hand will try to patch the devices it identified. It worked in the same way the Brickerbot did, by scanning the Internet for vulnerable IoT devices and then tries well-known ports such as Telnet and well-known password to login (Symantec, 2015). Once this is done the bot try to harden the security of the devices it had infected and then leave a message to the owner of the device to change the password (Symantec, 2014). The authors of the Wifatch bot did respond to Symantec stating that this project was created for four reasons: 1. learning experience 2. understanding 3. fun 4. security, both theirs and ours (Symantec, 2015).

These are two examples of how users have started to take actions on their own in order to improve security of the Internet. To make sure that mass DDOS options are not available like the Mirai botnet from the third ENISA example. Neither of the bots are legal either. The brickerbot of course as it did destroy the device it found but also the Wifatch bot. The reason is that it technically needs the permission of the owner of the devices in order to update the devices it found and did changes to. These are two good examples of what we can also start expecting more of unless IoT security starts to be taken seriously.

5.2 Jackware

A good way to explain what Jackware is to start by explaining what Ransomware is. Ransomware such as Locky or Cryptolocker are malicious software that will encrypt a user’s files and folders and keep them encrypted until a ransom is paid for them by the owner of the files or folders (Cobb, 2016).

Jackware is similar to ransomware but with a slight difference. Jackware will seek to control a device rather than the data of the device. The device in this case could be a smart car (Cobb, 2016). Jackware can lock down the car while the owner is in the car and will not unlock the car until a ransom is paid or even worse, start driving off on its' own and kidnapping the passengers of the car.

However, to this date July 2016 when the post was written, jackware was and hopefully still only is, theoretical (Cobb, 2016). Seeing how ransomware has started to spread in the form of Petya and NotPetya, jackware does sadly not seem like a dystopian future far away anymore. Instead it could potentially be something that we will see any day now unless security is taken seriously.

5.3 Project CHIP

As of December 2019 Amazon, Google and Apple among other companies stated that they are teaming up in order to create a new standard for smart home devices. With this new standard the devices can work with each other without any compatibility issues and it can potentially be applied to older devices as well (CHIP, 2019).

This project is named Connected Home over IP (CHIP) and the plans are to develop and adopt a royalty-free connectivity standard to increase compatibility among smart homes product and with security as a fundamental design (CHIP, 2019). The idea is to build upon the Internet Protocol (IP) with the shared belief that these devices should be secure, reliable and seamless to use together (CHIP, 2019).

Now one can finally see the industry trying to step up the game regarding IoT security, for smart homes at least. This standard is not locked down to the major players in the field but will be open anyone. They are planning on taking an open-source approach and using Github as the distribution platform so that anyone can use this method in the future which also will increase the security.

5.4 Tietoturva label

Another organization has opted to start providing a label for cybersecurity awareness. The organization is Traficom from Finland and the label can be applied for from https://tietoturvamerkki.fi/.

The idea behind the label is for manufacturers to be able to apply for and if approved they, once they have gone through testing, can use this label in marketing. It will show that their product has gone thru testing by Traficom and is secure. The label is only issued to products or services that meet the information security requirements set by the National Cyber Security Centre Finland at Traficom (Traficom, 2020). The label is a way to communicate security and responsibility and show that security is considered during the design (Traficom, 2020).

The fee for the test is 350€ per product or service that is submitted for auditing. The company shall also pay for the auditing of the device and services, however, the fee for this could not be found except that it was free during the pilot phase which was during autumn of 2019. Lastly, there is 350€ fee for the right to use the label.

Currently, as of February 2020 only three devices have applied for the label and passed the auditing and gained the right to use the Cybersecurity label. At least according to their site. These three devices are the Cozify Hub, a smart home hub, Polar Ignite workout watch and Wattinen, a smart thermostat. They are all Finnish devices, so no other nationalities have applied for the label or at least passed the tests or mentioned on their site.

In Figure 27 the newspaper Ilta Sanomat shows the Cozify hub and that they have passed the evaluation done by Tietoturva and that they have been approved the label. The label is clear and easy to notice and the QR code used in the logo will open the webpage https://tietoturvamerkki.fi/ if a user scans the logo so they can read up on what the label means.

Figure 27. Tietoturva label on Cozify (Ilta Sanomat, 2019)

6 CONCLUSION

The results and the study cases speak for themselves. Unless the users and the manufacturers do their part, IoT security will never improve. Users need to demand better security by making sure the products bought are designed with security in mind.

From a user perspective, this can be done simply by avoiding cheap knockoff devices and reading up about the products for before buying. Understandably, everyone buying an IoT device is not a security expert. Therefore, manufacturers need to improve on their part.

Manufacturers need to make sure they have security implemented.
Manufacturers need make sure security is kept simple but still have requirements like changing the default password on first login as an example. Another example is to make sure the devices are easy to patch and maintain if the customer has many devices.

This is the only way to improve security because unless it is not done there will be more copies of the Mirai botnet and brickerbots that will destroy the devices or maybe even highjack them similar to the jackware scenario. It should not matter if it is just a small toy or something big like car, security should always be implemented and should be an important part of the device. Just because the device cannot do any physical harm to anyone does not mean the device is not harmless in any other way. A hacker could potentially steal sensitive information in case security is not taken seriously.

By using the suggested guidelines and recommendations from this thesis, and maybe even building and expanding upon them, manufacturers can create secure yet easy to install and use IoT. Once the device has been created according to the guidelines and recommendations an evaluation can be done to confirm the device is secure.

REFERENCES

Akamai. 2018. UPnProxy: Blackhat Proxies via NAT Injections. Retrieved from https://www.akamai.com/us/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf [Accessed 24 November 2019].

Aruba. 2019. Internet of things. Retrieved from https://www.arubanetworks.com/solutions/Internet-of-things/ [Accessed 27 May 2019].

Ashton, K. 2009. That “Internet of Things” thing. Retrieved from https://www.rfidjournal.com/articles/view?4986 [Accessed 27 May 2019].

Cobb, S. 2016. Jackware: When connected cars meet ransomware. Retrieved from https://www.welivesecurity.com/2016/07/20/jackware-connected-cars-meet-ransomware/ [Accessed 3 January 2020].

Chu, G and Lisitsa, A. 2019. Penetration Testing for Internet of Things and Its Automation. Retrieved from https://www.researchgate.net/publication/330881119_Penetration_Testing_for_Internet_of_Things_and_Its_Automation [Accessed 12 April 2020].

Cimpanu, C. 2017. BrickerBot Author Retires Claiming To Have Bricker over 10 Million IoT Devices. Retrieved from https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/ [Accessed 26 December 2019].

CISOMAG, 2019. IoT cybersecurity bill introduced in Senate. Retrieved from https://www.cisomag.com/iot-cybersecurity-bill-introduced-in-senate/ [Accessed 23 April 2020].

ConnectedHomeIp. 2019. Project Connected Home Ip. Retrieved from https://www.connectedhomeip.com/ [Accessed 3 January 2020].

Core DNA. 2019. GDPR Explained in 5 Minutes: Everything You Need to Know. Retrieved from https://www.coredna.com/blogs/general-data-protection-regulation [Accessed 17 July 2019].

Council of the European Union. 2018. Interinstitutional File: 2017/0225(COD). Proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"). WWW Document. Available at: http://data.consilium.europa.eu/doc/document/ST-15786-2018-INIT/en/pdf [Accessed 17 July 2019].

Deloitte. IoT Innovation Report. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Internet-of-Things-Innovation-Report-2018-Deloitte.pdf [Accessed 16 June 2019]

ENISA. 2018. Baseline Security Recommendations for IoT. Retrieved from https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot [Accessed 4 September 2019]

ENISA. 2018. Baseline Security Recommendations for IoT. Retrieved from https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot [Accessed 4 September 2019]

European Commission. 2019. The Cybersecurity Act strengthens Europe's cybersecurity. Retrieved from https://ec.europa.eu/digital-single-market/en/news/cybersecurity-act-strengthens-europes-cybersecurity [Accessed 17 July 2019].

F-Secure a. 2019. Attack landscape H1 2019 Retrieved from https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf [Accessed 26 December 2019]

F-Secure c. IoT Threat Landscape. Retrieved from https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/04/01094545/IoT-Threat-Landscape.pdf [Accessed 28 May 2019]

Forcepoint. What is the CIA triad? Retrieved from https://www.forcepoint.com/cyber-edu/cia-triad [Accessed 17 June 2019].

Forcepoint. What is Cybersecurity? Retrieved from https://www.forcepoint.com/cyber-edu/cybersecurity [Accessed 17 June 2019].

Gaffney, T. 2019. Episode 27| The Connected Home Meets the IoT Tire Fire Retrieved from https://blog.f-secure.com/podcast-connected-home-iot/ [Accessed 23 September 2019]

Gartner. 2017. Leading the IoT. Retrieved from https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf [Accessed 16 May 2019].

Gallo, M. N. 2019. Senate Reintroduces IoT Cybersecurity Improvement Act. Retrieved from https://www.insideprivacy.com/Internet-of-things/senate-reintroduces-iot-cybersecurity-improvement-act/ [Accessed 17 November 2019]

Hassan. M. 2019. Senator Hassan Joins in Introducing Bipartisan Legislation to Improve Cybersecurity of Internet-of-Things Devices. Retrieved from https://www.hassan.senate.gov/news/press-releases/senator-hassan-joins-in-introducing-bipartisan-legislation-to-improve-cybersecurity-of-Internet-of-things-devices- [Accessed 17 November 2019].

Hern, A. 2018. Fitness tracking app Strava gives away location of secret US army bases. Retrieved from https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases [Accessed 25 May 2019].

Hyppönen, M. 2016. Twitter. Retrieved from https://twitter.com/mikko/status/808291670072717312 [Accessed 5 May 2020].

IBM. 2015. Point of View: Internet of things security. Retrieved from https://www.ibm.com/downloads/cas/7DGG9VBO [Accessed 27 May 2019].

INFOSEC. 2018. CIA Triad. Retrieved from https://resources.infosecinstitute.com/cia-triad/ [Accessed 17 June 2019].

Levi, R. 2017. Big Cannons. Retrieved from https://malicious.life/episode/episode-4-big-cannons-small-phish/ [Accessed 26 December 2019].

Kananen, J. 2015. Online research for preparing your thesis – A guide for conducting qualitative and quantitative research online 54, 61. Jyväskylä: Suomen Yliopistopaino Oy.

Kiss, J. 2014. Xbox live and PlayStation attack: Christmas ruined for millions of gamers. Retrieved from https://www.theguardian.com/technology/2014/dec/26/xbox-live-and-psn-attack-christmas-ruined-for-millions-of-gamers [Accessed 4 May 2020].

Miessler, D. 2015 IoT Attack Surface Mapping. Retrieved from https://www.youtube.com/watch?v=RhxHHD790nw [Accessed 7 July 2019].

Microsoft Threat Intelligence Center. 2019. Corporate IoT – a path to intrusion. Retrieved from https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/ [Accessed 15 August 2019].

NIST. 2017. About NIST. Retrieved from https://www.nist.gov/about-nist [Accessed 17 November 2019]

NIST. 2018. Cybersecurity Framework https://www.nist.gov/cyberframework [Accessed 15 December 2019]

NIST. 2019. Considerations for Managing Internet of Thing (IoT) Cybersecurity and Privacy Risks Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf [Accessed 17 August 2019].

NIST. 2019b. Core Cybersecurity Feature Baseline for Securable IoT Devices. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8259-draft.pdf [Accessed 15 August 2019].

Oxford Living Dictionaries a. Cybersecurity. Retrieved from https://en.oxforddictionaries.com/definition/cybersecurity [Accessed 16 May 2019].

Oxford Living Dictionaries b. Internet-Of-Things. Retrieved from https://en.oxforddictionaries.com/definition/Internet_of_things [Accessed 16 May 2019].

OWASP. 2020. About the OWASP Foundation. Retrieved from https://owasp.org/about/ [Accessed 05 May 2020]

OWAPS. 2019. Internet of things project. Retrieved from https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project [Accessed 05 May 2020]

Price, R. 2016. The smart-home device that Google is deliberately disabling was sold with a “lifetime subscription”. Retrieved from https://www.businessinsider.com/revolv-smart-home-hubs-lifetime-subscription-bricked-nest-google-alphabet-Internet-of-things-2016-4?r=US&IR=T [Accessed 3 June 2019].

Seals, T. Threatpost. CloudPets may be out of business, but security concerns remain. 2018. Retrieved from https://threatpost.com/cloudpets-may-be-out-of-business-but-security-concerns-remain/132609/ [Accessed 17 May 2019].

Shodan. What is Shodan? Retrieved from https://help.shodan.io/the-basics/what-is-shodan [Accessed 28 May 2019].

Steele, B. 2019. Tech Tuesday: Internet of Things (IoT). Retrieved from https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesday-Internet-of-things-iot [Accessed 12 January 2020].

Symantec. 2015. Is there an Internet-of-Things vigilante out there? Retrieved from https://www.symantec.com/connect/blogs/there-Internet-things-vigilante-out-there [Accessed 3 January 2020].

Traficom. 2020. Terms of Use – Cybersecurity label for IoT consumer devices. Retrieved from https://tietoturvamerkki.fi/files/iot-ttm-tems-of-use.pdf [Accessed 14 February 2020].

Verizon. 2015. Data breach Investigations Report. Retrieved from https://www.researchgate.net/publication/289254638_2015_Verizon_Data_Breach_Investigations_Report [Accessed 3 May 2020].

Whittaker, Z. 2017. Sonos says users must accept new privacy policy or device may “cease to function”. Retrieved from https://www.zdnet.com/article/sonos-accept-new-privacy-policy-speakers-cease-to-function/ [Accessed 12 January 2020].