A review on the Internet of Things

Ville Pulkkinen

2019 Laurea

Laurea University of Applied Sciences

A review on the Internet of Things

Ville Pulkkinen
Degree Programme in Business Information Technology
Bachelor's Thesis
November, 2019

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology
Bachelor's thesis

Ville Pulkkinen

A review on the Internet of Things

Year 2019 Pages 34

This thesis investigated and described the current state of the Internet of Things (IoT) from a security perspective. The goal was to present relevant information on the Internet of Things to consumers and businesses. The paper briefly explained what the Internet of Things is, how it can be applied in the real world, and at what capacity, and gave an overview of its current security landscape, threats, and vulnerabilities.

This paper had no practical research project, as it was purely an examination of the general state of the Internet of Things, presented in the form of a literature review. The study was conducted using publicly available research papers, newsletters, articles, books, blogs, and newsletters.

The conclusions of the thesis show that the Internet of Things and its security is still mostly un-standardized, as there is such a numerous amount of use-cases for IoT devices, and an all-encompassing solution to security does not exist as of now. However, device vendors and cybersecurity companies are working to secure their solutions to protect their own, and others' IoT devices. Regulators around the world are also trying to create a set of rules and regulations to keep the Internet of Things safe, for the benefit of everyone.

Keywords: internet of things, security, threats, vulnerabilities

Laurea-ammattikorkeakoulu	**Tiivistelmä**
Tietojenkäsittely	
Tradenomi (AMK)	
Liiketalouden ammattikorkeakoulututkinto	

Ville Pulkkinen

Artikkelikatsaus esineiden internetistä

Vuosi	2019	Sivumäärä	34

Tässä opinnäytetyössä tutkittiin ja kuvailtiin esineiden internetin nykytilannetta tietoturvan näkökulmasta. Tavoitteena oli tuoda esille oleellista tietoa esineiden internetistä kuluttajille sekä yrityksille. Työ selittää lyhyesti mikä esineiden internet on, kuinka sitä voidaan soveltaa todellisessa maailmassa ja missä kapasiteetissa, sekä antaa yleiskuvan sen turvallisuuden nykytilasta, sekä haavoittuvuuksista ja heikkouksista, yleisten uhkien ja haavoittuvuuksien määrittämiseksi sekä niiden löytämiseksi ja niiltä suojaamiseksi.

Opinnäytetyössä ei ollut toimeksiantajaa, sillä se oli puhtaasti esineiden internetin yleistilanteen tutkimista, joka esitettiin kirjallisuuskatsauksen muodossa. Tutkimus toteutettiin käyttämällä julkisesti saatavilla olevia tutkimuspapereita, uutistiedotteita, artikkeleita, kirjoja, blogeja, sekä tiedotteita.

Työn johtopäätökset kertovat, että esineiden internet ja sen tietoturva on vielä laajalti standardoimaton alue, sillä IoT-laitteiden käyttötapauksia on niin suuri määrä, että yhtä kaikenkattavaa ratkaisua ei ole. Laitetoimittajat kuitenkin työskentelevät ratkaisujensa turvaamiseksi omien ja muiden Internet-laitteiden suojaamiseksi. Sääntelyvirastot ympäri maailmaa yrittävät luoda joukon sääntöjä ja määräyksiä pitääkseen Internet turvallisena kaikkien hyödyksi.

Asiasanat: esineiden internet, tietoturva, heikkoudet, haavoittuvuudet

Table of Contents

1 Introduction

In this thesis, I present information from my research on the Internet of Things: how it’s applied in the real world, and its current status from a security-focused standpoint. The Internet of Things is the concept of connecting nearly any device that has an on/off switch to the Internet and each other. These kinds of devices include smartphones, wearables (such as smartwatches), coffeemakers, lightbulbs, refrigerators and washing machines, and nearly anything else that one can think of. This kind of connectivity also applies to components in industrial machinery, such as the mechanical arm in a vehicle assembly line.

IoT is quickly becoming a part of everyday life, be it in households, businesses, industry, or in services, as it can be applied to the simplest household electronics to massive industrial operations or even healthcare, such as in monitoring patients. As a continually increasing number of devices are becoming connected every day, security threats are always looming nearby.

There is a large number of competing technologies and organizations in the IoT industry, as IoT covers a wide range of applications that require devices and technologies with different feature sets.

2 Thesis background

My first introduction to IoT was during the early days of my studies in 2016 when the topic was briefly touched upon during a lecture. I have been very interested in IoT ever since, as the idea of an interconnected world piqued my interest. This interest eventually led me to choose it as my thesis topic back in 2018.

This thesis is not a practical research project but rather a literature review presenting information about the Internet of Things, its information security, vulnerabilities, and useful information for individuals or organizations. I chose to write my thesis this way instead of a commissioned project for an organization, as I find it easier and more comfortable researching and working on a project on my own.

2.1 Research methods

The research method used to analyze the information found was document analysis. In this research method, the researcher studies documents to give meaning to the chosen topic by examining it from various viewpoints and writing down the results (Bowen 2009, 27-40). I decided to select document analysis as a research method due to its characteristic of studying a topic from different viewpoints.

The disadvantages or potential limitations of document analysis are that documents are not always created with data research in mind, and therefore may require some investigation expertise. A given report or text might not provide the researcher all of the data they need, and other documents may only offer a small amount or even none at all. The material being researched can also be incomplete, with a crucial part of information missing. (Bowen 2009, 27-40).

Additionally, one should be aware of the possible existence of biases when analyzing documents. These can be present in both the source material and the researcher, so thorough evaluation and investigation of the subjectivity of documents, and understanding the data to preserve the credibility of the research at hand is essential. (Bowen 2009, 27-40).

Qualitative research means a type of scientific research that consists of an investigation that has some distinct characteristics, it:

- seeks to discover an answer to a question
- uses predefined procedures to answer the question
- collects evidence
- yields findings that are not determined in advance
- yields findings that can be used beyond the direct boundaries of the study

Qualitative methods are useful in identifying different factors, such as socioeconomic status, gender roles, and ethnicity. When used aside quantitative methods, qualitative research can help to interpret and better understand the reality of a given situation and the insinuations of quantitative data. Furthermore, it seeks to follow a specific research topic or problem from the different perspectives of the local population it involves. (Mack et al. 2005).

Zina O’Leary (2018) outlines a 10-step process for researching a chosen topic, which I used during my research. Recognizing these steps was an essential part of collecting data and understanding my subject better. The steps are:

- Curiosity
- Question development
- Understanding the state of play
- Revise & hone in

- Deciding where the answers are found
- Deciding how to collect data
- Getting the data together
- Making sense of the findings
- Sharing insights
- Offering recommendations

Curiosity in the chosen topic is essential, as asking how things work and questioning why they cannot be better is how a research process often starts. Once interests are found, one should find some pertinent research questions. In my case, I had 3 research questions that I wanted to find an answer to in my work. Once these questions are written down, finding out what others have already researched on the topic is a good idea, as doing work that has already been done is not ideal.

After this, the next step is finding out where the answers to the research questions may lie. Is it with a panel of experts on the topic, in documents, on the web, or perhaps on existing records? I found my answers mostly on the internet, as companies and organizations in the IT-industry have plenty of useful data and information available on my chosen topic. Data collection and analysis is the next step, in which data from found sources is collected and trawled through to see the pertinent pieces of information for the research.

Analyzing collected data is an ongoing process that continues throughout the entire research process, and during it, one should look for meaning in the information that has obtained. I used over 25 different sources of information, such as industry research reports, website articles, expert blogs, and marketing material, to create a stronger base of knowledge by using multiple sources.

Because of the many sources I had, some analysis was required to cut out marketing hype and to find the best source for a particular piece of information if I found it in multiple sources. I chose sources based on research into the company or individual that published the article or blog in question to make sure that they are a reputable name in their industry. If any information on their reputability or products was not found, or they had poor feedback online, I did not choose them as a source. In some cases, the information had to be sought out from the website of the developer of a specific technology or service, or from materials where external research was not available. Being cautious about this kind of information is a good idea, as companies tend to sell their own products.

2.2 Research objectives

The objective of this thesis is to answer the following questions:

- What is the Internet of Things, and how can it be applied in the real world?
- Why is security of the utmost importance when dealing with the Internet of Things?
- How can consumers and enterprises improve their IoT security, based on my findings?

2.3 Terms

ARC – Argonaut RISC Core. Embedded 32-bit processors used in SoC devices

DDoS - Distributed denial-of-service attack

GUI – Graphical user interface

IIoT – Industrial Internet of Things

JTAG - Joint Test Action Group, a standard for design verifying and circuit board testing

RFID – Radio-frequency identification, a method for identifying and tracking tags in objects

SoC – System on a chip, an integrated circuit that integrates all components of a computer

SWD – Serial Wire Debug, an electrical alternative JTAG interface

TTY – Teletype, more commonly known as a terminal

UART - Universal asynchronous receiver-transmitter

UPnP – Universal Plug and Play, a set of network protocols that lets devices seamlessly discover each other

WEP – Wired Equivalent Privacy, a security protocol for WLAN networks

WPA – Wi-Fi Protected Access, a security protocol for WLAN networks

3 The IoT and the hype around it

In the modern-day, more and more devices are becoming connected to the internet. These kinds of devices include ones that you might think; smartphones, smartwatches, laptops, and televisions - but also things such as light bulbs, refrigerators, and even toasters. An all-encompassing list of IoT devices is impossible to define, but instead, one must think that nowadays, any device that uses an existing communications protocol has the potential to be an IoT device. The IoT is remarkable in the sense that it has the ability to scale from the smallest applications to large ones, e.g., from a smartwatch to a fleet of self-driving cars (Cisco 2011). Figure 1 illustrates IBM's model for the Internet of Things, where different "things" can be seen along with an example of a connection model via cloud services.

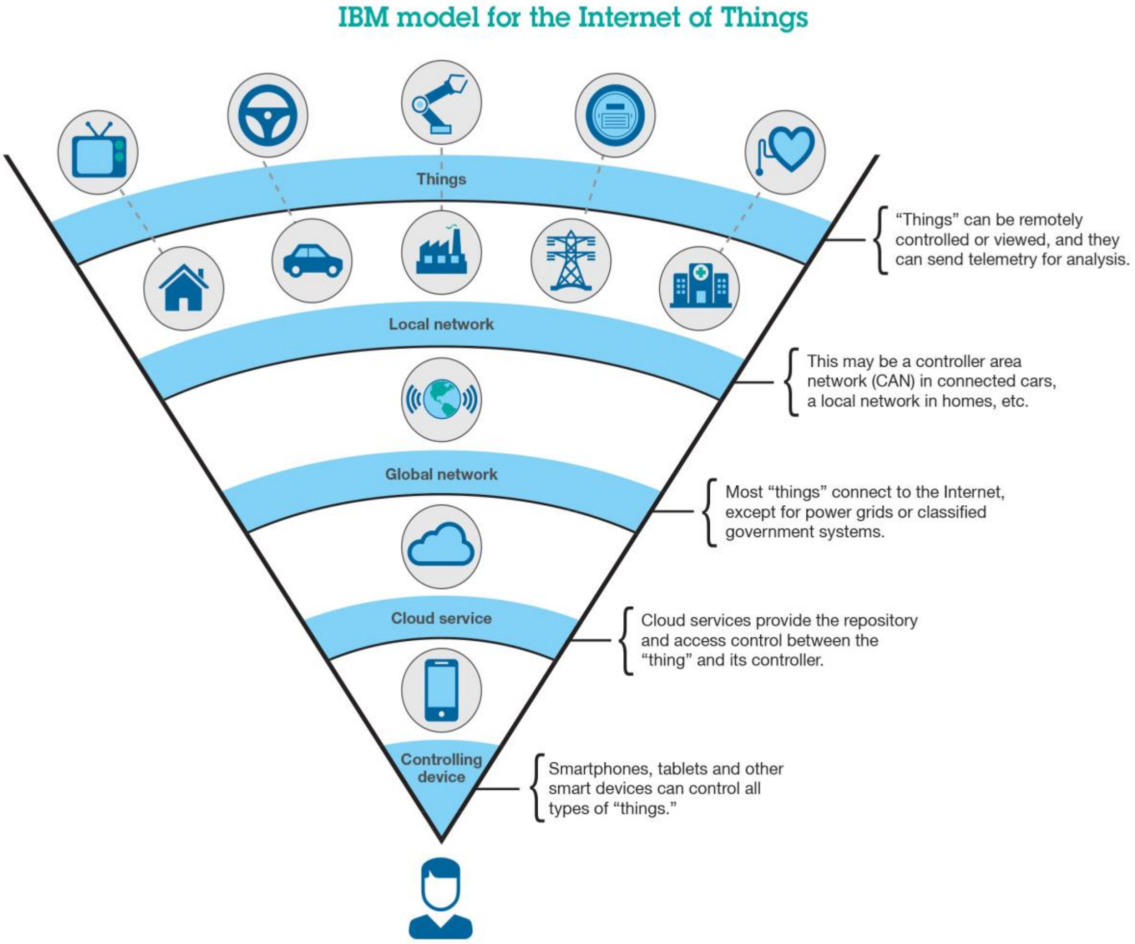

IBM model for the Internet of Things
Things
"Things" can be remotely controlled or viewed, and they can send telemetry for analysis.
Local network
This may be a controller area network (CAN) in connected cars, a local network in homes, etc.
Global network
Most "things" connect to the Internet, except for power grids or classified government systems.
Cloud service
Cloud services provide the repository and access control between the "thing" and its controller.
Controlling device
Smartphones, tablets and other smart devices can control all types of "things."

Figure 1: IBM model for the Internet of Things (IBM 2015)

Keen IoT supporter Cisco (2011) has confidence that the IoT will be responsible for 50 billion devices being online and connected to the Internet by the year 2020. Other companies such as General Electric (2019, 2) and Gartner (2016) have interest in the field; however, they have a more conservative forecast on the short term growth and financial potential of the IoT

– with their estimates being 20-25 billion devices and 1.9 trillion dollars spent by the year 2020. (Gilchrist 2017, 6).

While the IoT market is continually growing, many perceive that consumer adoption is lagging when compared to market potential. This can be a result of many different factors, like the ease of use, consumer distrust, or security concerns. IoT For All (2019) states that the top three factors that are affecting the lag behind consumers adopting IoT technology are feasibility, reliability of connection between devices, and the functionality of the devices themselves.

That being said, not everyone in the technology industry shares mutual confidence in the potential of IoT. Some are unconvinced since the IoT has been around in some capacity since even before the year 2000 but has been hyped a lot in recent years. According to the research and advisory company Gartner (2016), the hype for IoT has been at its peak for some years now. While many agree that the hype is high, others believe that issues over things like poor security, consumer trust, and privacy concerns will inhibit growth (Gilchrist 2017, 6). Figure 2 illustrates Gartner’s hype cycle for the Internet of Things.

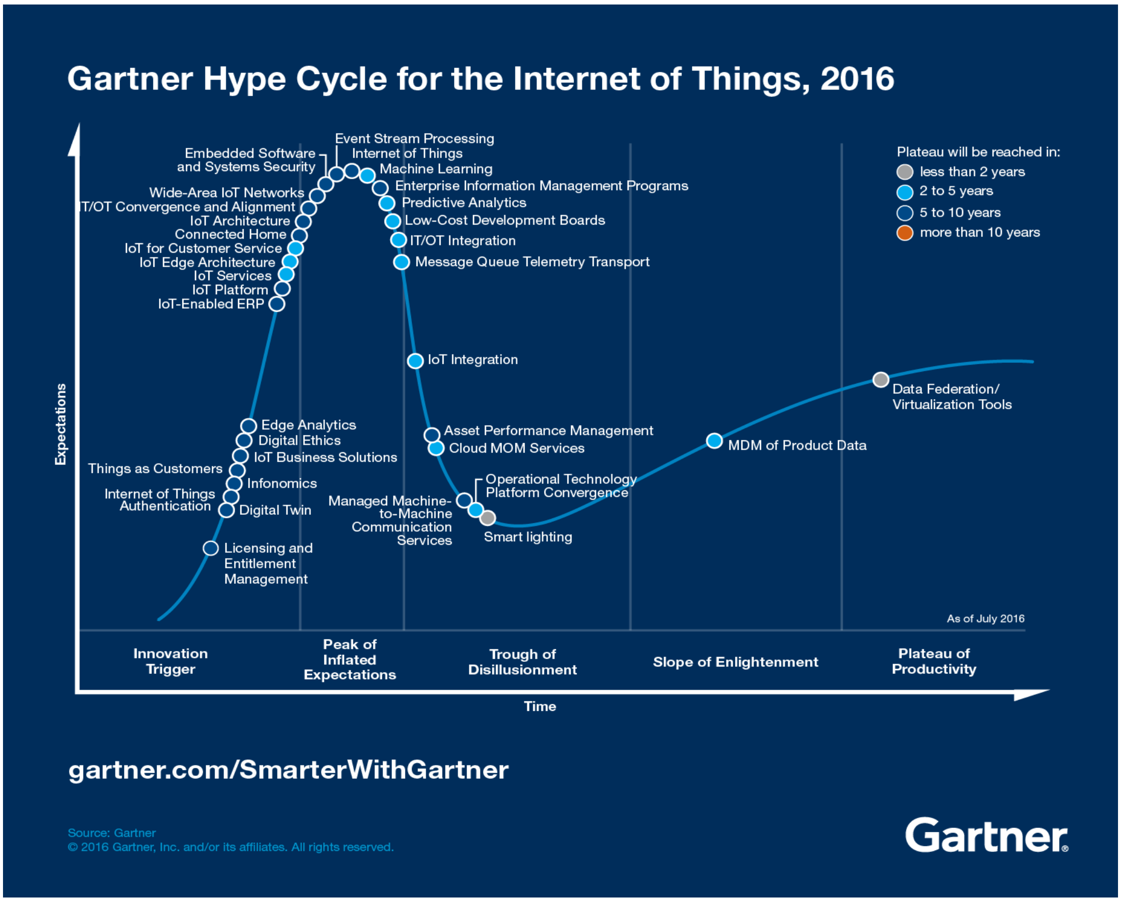


Figure 2: The hype cycle for IoT (Gartner 2016)

On the security side of things, according to the IoT Security Foundation (2018), hopes that security-conscious consumers begin creating a demand for IoT devices with better-implemented security have yet to materialize. Some believe that a split approach to a lack of security standards and product security features can risk lessening market confidence and stifling market potential. (IoT Security Foundation 2018).

3.1 IoT applications

Applications for IoT are found almost anywhere, and this chapter discusses a few examples that are already found in the real world. From consumer-based applications such as wearables like smartwatches, smart TVs, and thermostats to more industry-focused ones such as driverless forklifts, IoT is expected to equip billions of objects in the near future with intelligence and connectivity for improved efficiency, performance and analytics, and to overall enhance or automate some parts of the everyday lives of people around the world. (Arm 2019).

While IoT applications are seemingly limitless, several vital markets have begun emerging as areas where it seems likely that they will scale first, which will start offering some significant benefits to consumers and businesses there. These initial IoT markets can serve as testing grounds for companies, research organizations, and IoT developers, as here they may explore the numerous possibilities that IoT can deliver. (Arm 2019).

3.1.1 Supply chain

IoT hopes to improve supply chain logistics by enabling the managing of goods along every step of the way within a particular logistics network. According to Sigfox (2019), missteps along supply chains are unavoidable. No matter how robust the logistics network is for a product or asset, as at some point, something can and will go wrong. This can range from things like a truck getting stuck in traffic, to an asset going missing. Traditional supply chain management solutions may not catch on to missing, delayed, or misrouted assets until the product arrives hours late, or doesn’t arrive at all. While RFID tags are currently used to improve supply chain management in the form of asset tagging, this does not give information as to what is happening in between destinations, which can leave whoever is in charge in the dark about the current state of whichever product they are moving (Sigfox 2019).

By using IoT technology, smart solutions in logistics can change the way that modern supply chains work, as for the first time, the logistics industry may visualize and efficiently manage the delivery and handling of goods on a global scale from anywhere, at any time, using real-time asset tracking (Sigfox 2019), with many companies reportedly already using, or considering the use of IoT technologies in order to streamline their supply chain (APQC 2016). Figure 3 shows a chart of organizational use of IoT technologies in streamlining the supply chain, as an illustration of a survey by APQC in 2016.

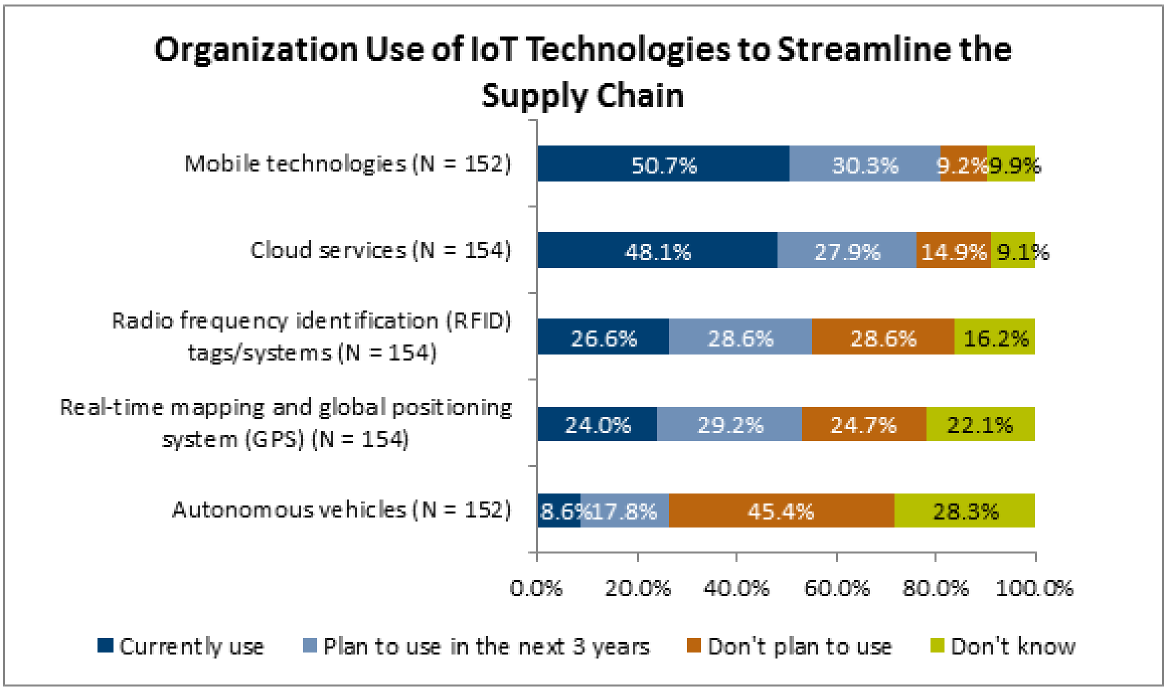


Figure 3: IoT uses in streamlining the supply chain (APQC 2016)

3.1.2 Smart home

A smart home refers to a home or household responding to nearby actions and changes, such as in the case of smart thermostats, which can adjust their temperature depending on the user’s preference, or independently by using machine learning. (Bhat, O., Bhat, S. & Gokhale 2017). Figure 4 illustrates a model of a home with ideal smart home features.

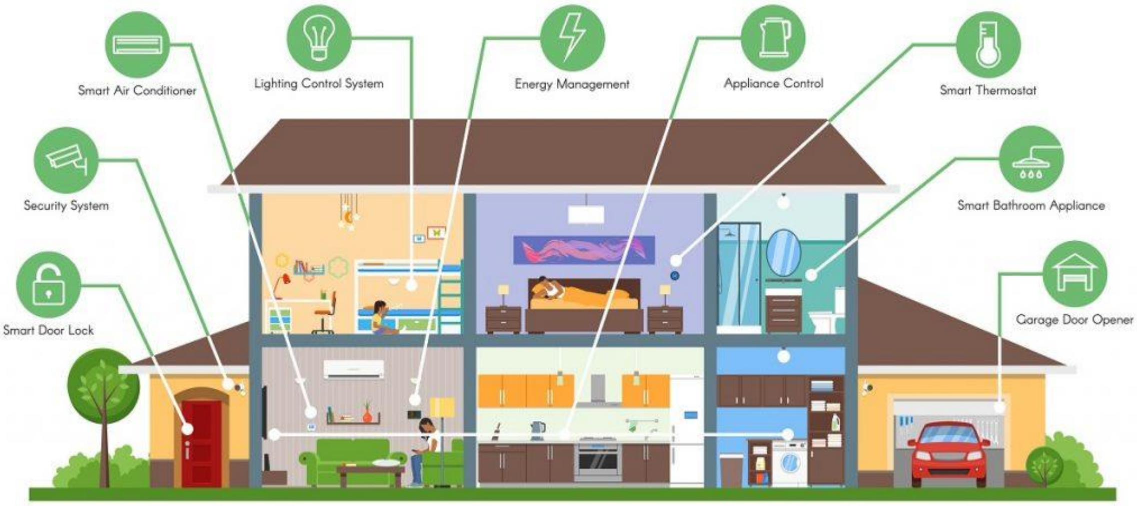


Figure 4: Ideal smart home features (Security Alliance 2016)

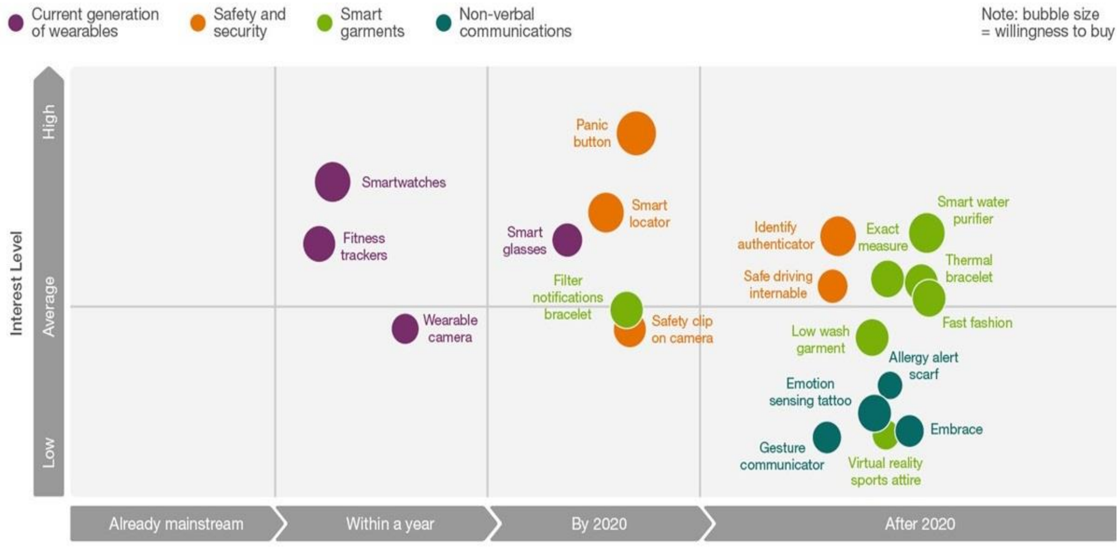
Third generation Nest smart thermostat devices use machine learning algorithms to continually monitor the temperature in order to get a good reference figure. This reference temperature data provides the thermostat with information such as what a person’s schedule is like, what kind of temperature settings they prefer, and at what time of day. Sensors in the premises and GPS information from the user’s mobile device is used to let the device know when the user is home and when they are away, which allows the device to dial in a suitable temperature for the user while they are home, and to dial back on heating or cooling while the user is gone, in order to conserve energy. (Bhat, O et al. 2017).

Smart home systems require many components to function and to connect to the Internet. These include sensors, processors, software, actuators, and databases. Sensors collect internal and external data from the household, continually measuring the conditions. These sensors are physically connected to the home itself, and to any devices that need sensor data. Processors perform integrated and local actions and may be connected to the cloud for applications that necessitate extended resources. Sensor data is then handled by server processes locally. Actuators are components such as switches and motors, which can perform various actions, such as adjusting an operational system or turning things on or off. Databases store unprocessed data collected from sensors or processed data received from cloud services. (Domb 2019)

3.1.3 Wearables

Wearable devices with IoT capabilities, e.g., fitness trackers and smartwatches, are typical examples of IoT technology being used in everyday life. They mainly have singular functions, such as exercise tracking or keeping time. According to IoT For All (2019), wearables have not fully penetrated the consumer market yet, but they do have an exciting future in healthcare monitoring.

Currently, wearable health and fitness devices are identified as the first step toward the future of wearable IoT devices. Right now, consumers are hopeful that in the future, wearables can not only be health and fitness tracking related personal devices but rather much more. The consensus is that the wearable technology mass adoption point is beyond 2020 because of uncertainty on whether the wearable industry has found the use cases that will lead to mass adoption (Ericsson 2016). Figure 5 shows Ericsson's survey results, where the inflection point is situated after 2020.

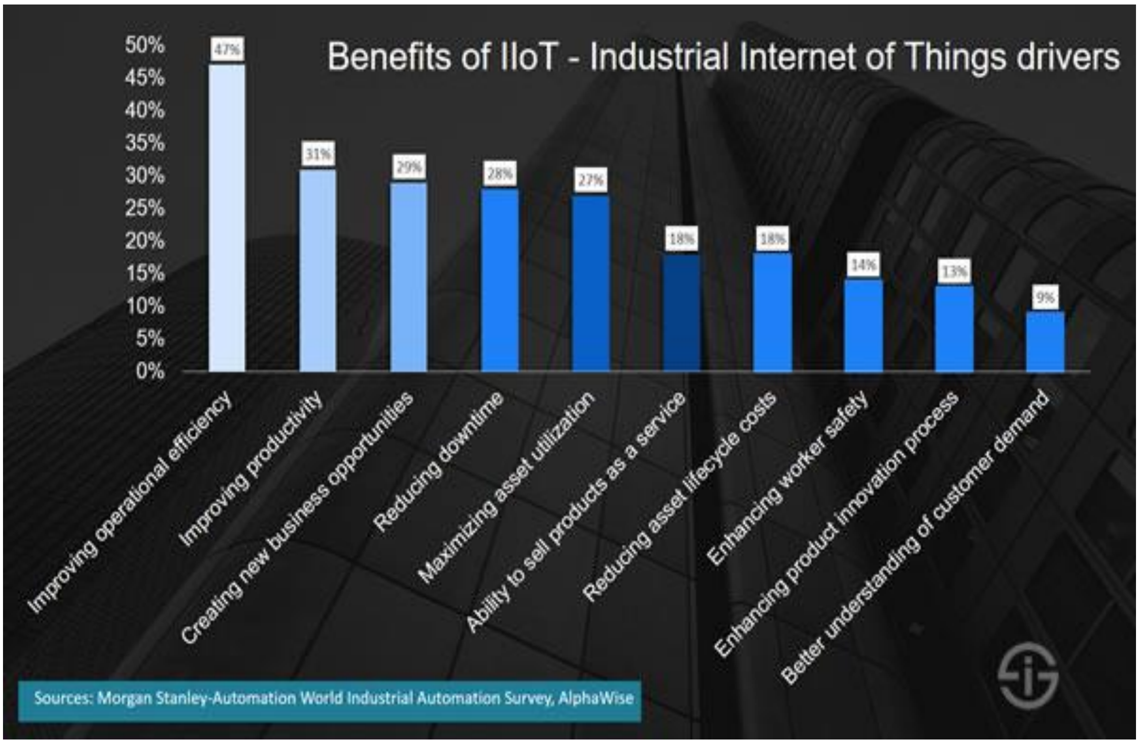


Source: Ericsson ConsumerLab, Wearable Technology and the Internet of Things, 2016
Base: Smartphone users across Brazil, China, South Korea, UK and the US

Figure 5: Consumers predict wearable inflection point to be beyond 2020 (Ericsson 2016)

3.1.4 IIoT

The Industrial Internet of Things helps bring together machines, people, and analytics in different industries. It is a network of industrial devices linked together by communications technologies, with the end product being systems that can gather, monitor, and analyze data, and provide useful new insights to companies. According to GE Digital (2019), these new insights can help lead industrial companies to make smarter business choices. In figure 6, i-SCOOP illustrates some benefits that IIoT.



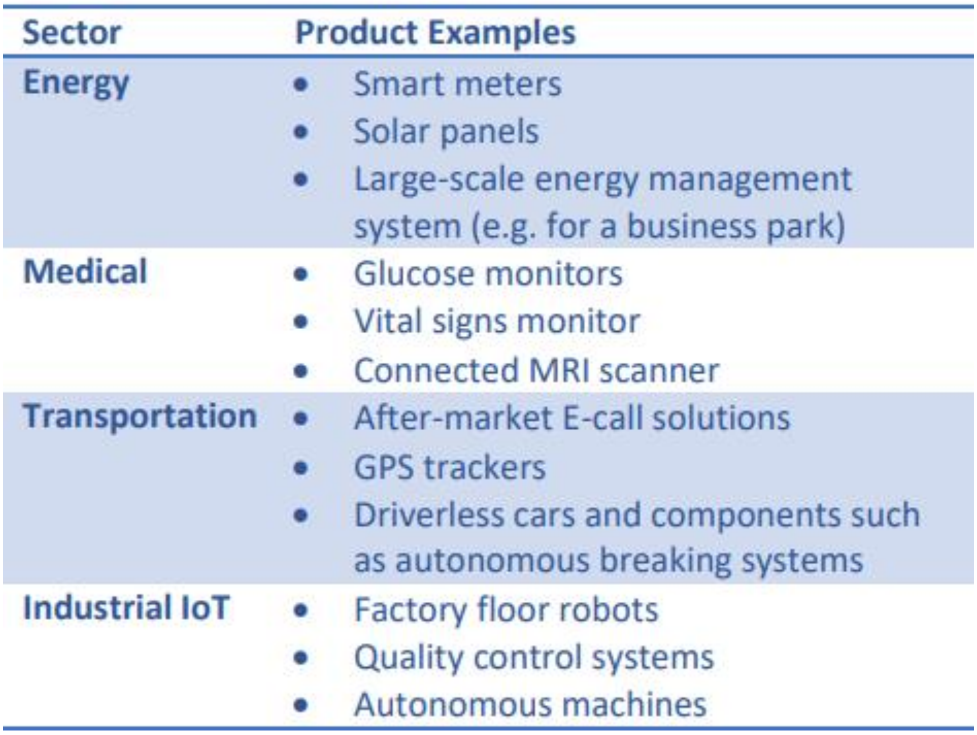
Sources: Morgan Stanley-Automation World Industrial Automation Survey, AlphaWise

Figure 6: Benefits of IIoT (i-SCOOP 2018)

3.2 Current regulations around IoT

Security is a journey, not a destination. It continuously moves forward and evolves with technology, and a security-focused mindset can support providers of IoT services and products in mitigating risks quite a lot, which can range from regulatory action to cybersecurity vulnerabilities and threats. Companies must be ready to support their products for the extent of this journey. Implementation of best security practices, for example, the ability to patch and update their product will not only help them withstand cyber-attacks but also contribute to regulatory compliance and mitigation of corporate liability. IoT is a substantial opportunity for society and businesses around the world, but if not suitably secured, it can also pose safety, privacy, and security risks to users, data, and information systems. The effect of these threats can range from negligible inconveniences to severe data breaches and financial losses. With these concerns in mind, regulators have acted and applied sanctions against IoT providers, relying on existing laws. As a result, there are numerous issues that suppliers need to be mindful of within each jurisdiction. Unfortunately, holes in regulation and resulting changes to guidelines are often apparent only *after* something goes wrong. (IoT Security Foundation 2018).

The regulations around IoT are likely to have some changes in the coming times. As of 2018, national or regional level regulations relevant to IoT have yet to be ratified. However, regulatory agencies and governments in the US, the EU, and the UK are considering or already developing new regulations specific to IoT and its security. As of the time of writing, the general expectation is that reputable IoT providers and vendors will adopt, and legislators will support outlines for compliance, or frameworks to establish satisfactory compliance with regulations (IoT Security Foundation 2018). Figure 7 is a table of business sectors where security compliance requirements relating to IoT are expected to appear in the coming years. This is not based on upcoming regulations, instead provided for illustration as to where new legislation changes are most likely to happen.



Sector	Product Examples
Energy	• Smart meters • Solar panels • Large-scale energy management system (e.g. for a business park)
Medical	• Glucose monitors • Vital signs monitor • Connected MRI scanner
Transportation	• After-market E-call solutions • GPS trackers • Driverless cars and components such as autonomous breaking systems
Industrial IoT	• Factory floor robots • Quality control systems • Autonomous machines

Figure 7: IoT product examples (IoT Security Foundation 2018)

Different industries beginning to adopt IoT technology should be proactive in taking a security-first mentality to start acclimatizing to a continually developing landscape in terms of regulations and legislature. Those with this security-first mentality should bear in mind the design, production, operation, and the entire lifecycle of their IoT services and products, which will support compliance with regulations while demonstrating that their company truly cares about their customers and their security while reducing the risk of non-compliance. Adapting a security-first approach will also improve the baseline security of IoT services and products in different marketplaces and will likely help safeguard against some risks associated with legacy devices (IoT Security Foundation 2018).

4 Security

While IoT technology brings many significant benefits to end-users, it also carries with it some unprecedented challenges in security. A considerable problem with IoT devices is their often-lax security. The manufacturers' liability for a product often expires after the warranty period, and interest in maintaining the equipment may stay small. A big question right now is how can the security of IoT devices be improved, and what should be considered in doing so?

Information security, in general, is based on three principles: Confidentiality of information, Integrity of information, and Availability of information. Confidentiality means the need to keep the information secret from outside eyes when needed, which is often achieved by only using a password. Integrity means that the sent message remains untampered, and different kinds of encryption methods ensure this. Access to information means that only the right people have access to certain information. Many security features are designed to safeguard one or more facets of this so-called CIA triangle. (Whitman & Mattford 2012).

The high growth rate of IoT devices is a new challenge for maintenance personnel of IT-systems. It also puts pressure on network operators to reform their infrastructure to withstand this new, more significant data stream that comes with IoT. When different smart devices, computers, and sensors are all connected to the same data network, they can become challenging to manage and adequately secure. When it comes to a new device that connects to an extensive data network, it is essential to first test in a smaller operating environment. Thus, a recommendation for companies looking to adopt IoT into their operations is to start launching new IoT devices as small-scale pilot projects. (T-Systems 2019).

From a household IoT-application standpoint, an important question for consumers is whether connecting a device such as a toaster or a refrigerator to the home network is necessary. One should look at the benefits and downsides of having a network-connected home appliance and then make the decision accordingly. One solution for household IoT security is to create a separate wireless network for IoT devices to operate on. For IoT device settings, it is vital to create strong passwords, so that the most straightforward external attack, guessing a password, is prevented. Additionally, turning off any UPnP features within the IoT network is a good idea. One should also check that the IoT device has the latest firmware update from the manufacturer. Care should be taken when connecting an IoT device to a network that deals with cloud services, as an external device can provide an easy path for a malicious party. (Norton 2019).

In the end, users of IoT devices should have at least reasonable IT skills to keep their network and devices safe. Alternatively, the device manufacturer or service provider should create a robust set of instructions for the end-user, so that they can maintain a stable level of security without it being too complicated. The worst-case scenario is that the device manufacturer has not even given the user the option to change the default password, which shouldn't ever happen.

4.1 Defense in depth

According to IBM (2015), one successful method of defending against threats to an IoT system is to implement techniques that employ so-called "defense in depth"- techniques. Defense in depth means that security mechanisms are added at various points in the system to enhance security. The purpose of this is to ensure the integrity of the system, even if any security-enhancing component fails. When employing defense in depth techniques, different security protocols should be implemented in different parts of the system, such as device, firmware, and device-to-cloud communication. IBM's IoT system chart in Figure 8 below illustrates the areas of IoT that should be kept in mind when it comes to implementing proper IoT system security, which includes the data itself, the data collectors, applications, gateways, and IoT devices themselves.

If every aspect is not taken into consideration, just one security issue in certain areas can significantly compromise overall system security. For example, with weak communication encryption, an attacker can retrieve a username and password from network traffic and use them to identify themselves to the system.

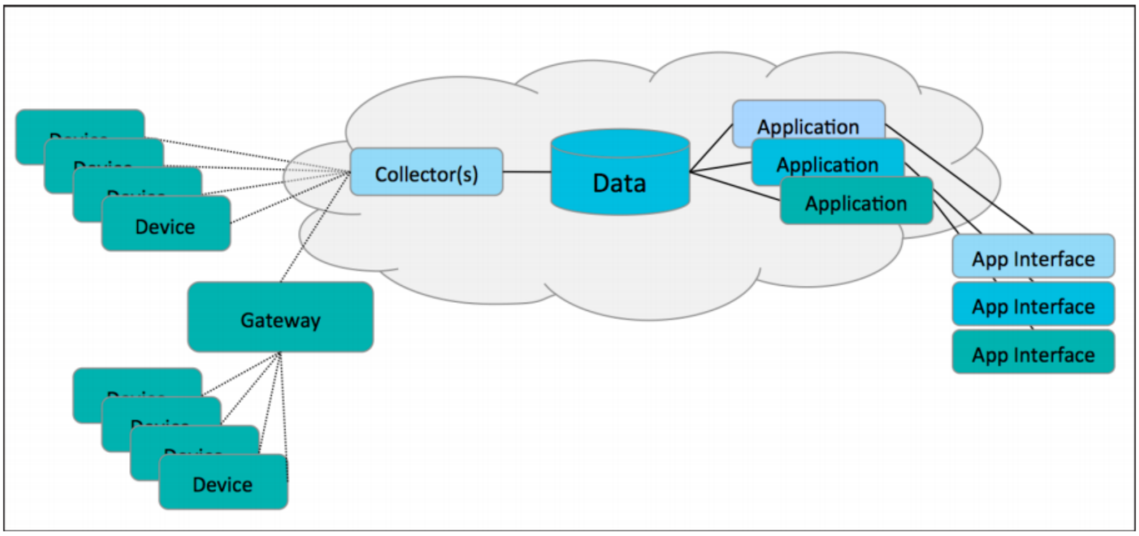


Figure 8: IBM IoT system chart (IBM 2015)

4.2 Testing security

Implementing security is not enough by itself, as a system is only as secure as its weakest link. Therefore, the security of a system should be tested in order to find weak spots. In IoT devices and networks, security can be tested in various different ways. For example, devices can be attacked from outside the network they are operating on by using different kinds of tools and software, and professionals in the IT industry are the primary users of these kinds of tools. In IoT devices, many ports are often accessible from outside the network, which can give malicious parties easy access to the device, and from there, even an entire network. By testing for vulnerabilities, possible intrusion points can be found and closed. (Cloudflare 2019).

4.2.1 Penetration testing

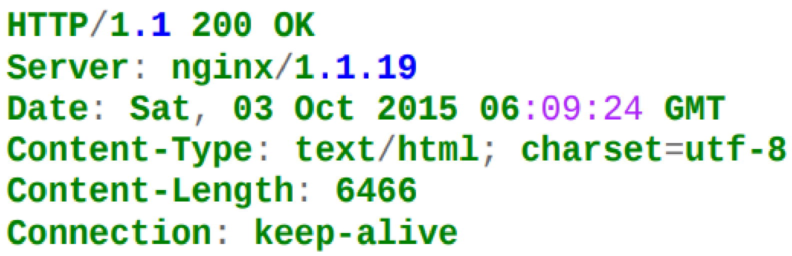
Penetration testing (or pen testing) is the application of ethical hacking, by employing a simulated cyber-attack, to find and exploit security vulnerabilities in a device, or even an entire network. The aim of this is to find weaknesses before malicious parties do. Pen tests are best performed by outside contractors who have no prior knowledge of an organization’s network or systems, as they may be able to uncover blind spots in security. These pen-testing contractors are commonly referred to as ethical hackers (Cloudflare 2019). Testing only Ethernet-based technologies can increase the risk of missing some vulnerabilities in wireless connections. Companies use various other radio frequencies outside the standard 802.11 protocols for various reasons, thus facilitating the need for changes in testing tools. (The Register 2017).

In IoT, penetration tests can be executed on the following elements of a device: ports (UART, SWD, & JTAG), flash memory chips, and buses. Exposed ports such as a serial port are used by pen testers to gain root access and for viewing sensitive data, while flash memory chips allow a possibility to dump firmware onto the device, and buses may be sniffed for possible cleartext data that can include confidential information (InfoSec Institute 2018). A popular piece of pen testing software with IoT-testing capabilities is Metasploit. Metasploit is used in probing for IoT-related weaknesses in different environments, and according to its publisher Rapid7 (2017), its radio frequency testing-component, RFTransceiver grants teams greater visibility of foreign IoT devices. Rapid7 (2017) states, "The importance of RF testing will continue to escalate as the IoT ecosystem further expands."

4.2.2 Shodan

Different search engines available to specialists and non-specialists alike can map network devices that are open to the outside. Shodan is an example of a network device search engine that finds devices connected to the Internet. Unlike web search engines such as Bing or Google, Shodan lets users search for devices and different kinds of information about those devices. Things such as how many anonymous FTP servers exist, how many hosts a new type of virus is capable of infecting, or even what software a specific device is running. (Matherly, J 2016).

Shodan gathers and represents data in banners. These are printouts of text which describe a service on a device. Using web servers as an example, these are the headers that are returned as a result of a search. The data contained in these banners vary depending on the type of service that it was gathered from. For example, an HTTP banner might include information about the webserver that it runs on.

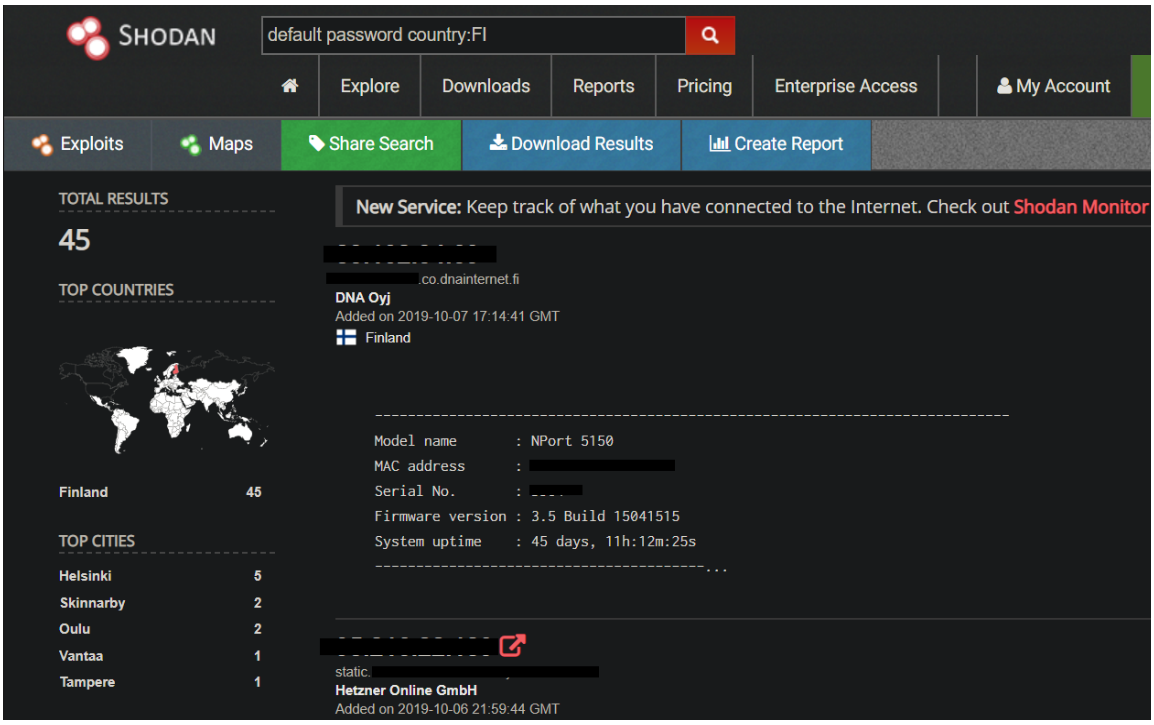


```
HTTP/1.1 200 OK
Server: nginx/1.1.19
Date: Sat, 03 Oct 2015 06:09:24 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 6466
Connection: keep-alive
```

Figure 9: Typical HTTP banner (Matherly, J 2016)

Alongside banners, Shodan also gathers metadata about devices, which includes things such as the hostname, operating system, or even the geographic location. Most of this metadata can be searched for via the Shodan website, although some options are only available to developers and other API users. (Matherly, J 2016).

People are often unaware of the security of their devices. Many, for example, leave the passwords of their devices to default ones set by the device manufacturer, and Shodan can find such network-connected devices with ease. More security-conscious people, however, can test the security of their devices by utilizing Shodan. Due to its powerful nature, it can be a very dangerous tool in the hands of the malicious people, as it can easily find devices that have gaping holes in their security—and this includes IoT devices. Figure 10 illustrates a Shodan search for devices in Finland that have a default password.



TOTAL RESULTS

45

TOP COUNTRIES

Finland	45

TOP CITIES

Helsinki	5
Skinnarby	2
Oulu	2
Vantaa	1
Tampere	1

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

[redacted]

[redacted].co.dnainternet.fi

DNA Oyj

Added on 2019-10-07 17:14:41 GMT

Finland

```
--------------------------------------------------------------------------------
Model name       : NPort 5150
MAC address      : [redacted]
Serial No.       : [redacted]
Firmware version : 3.5 Build 15041515
System uptime    : 45 days, 11h:12m:25s
----------------------------------------...
```

[redacted]

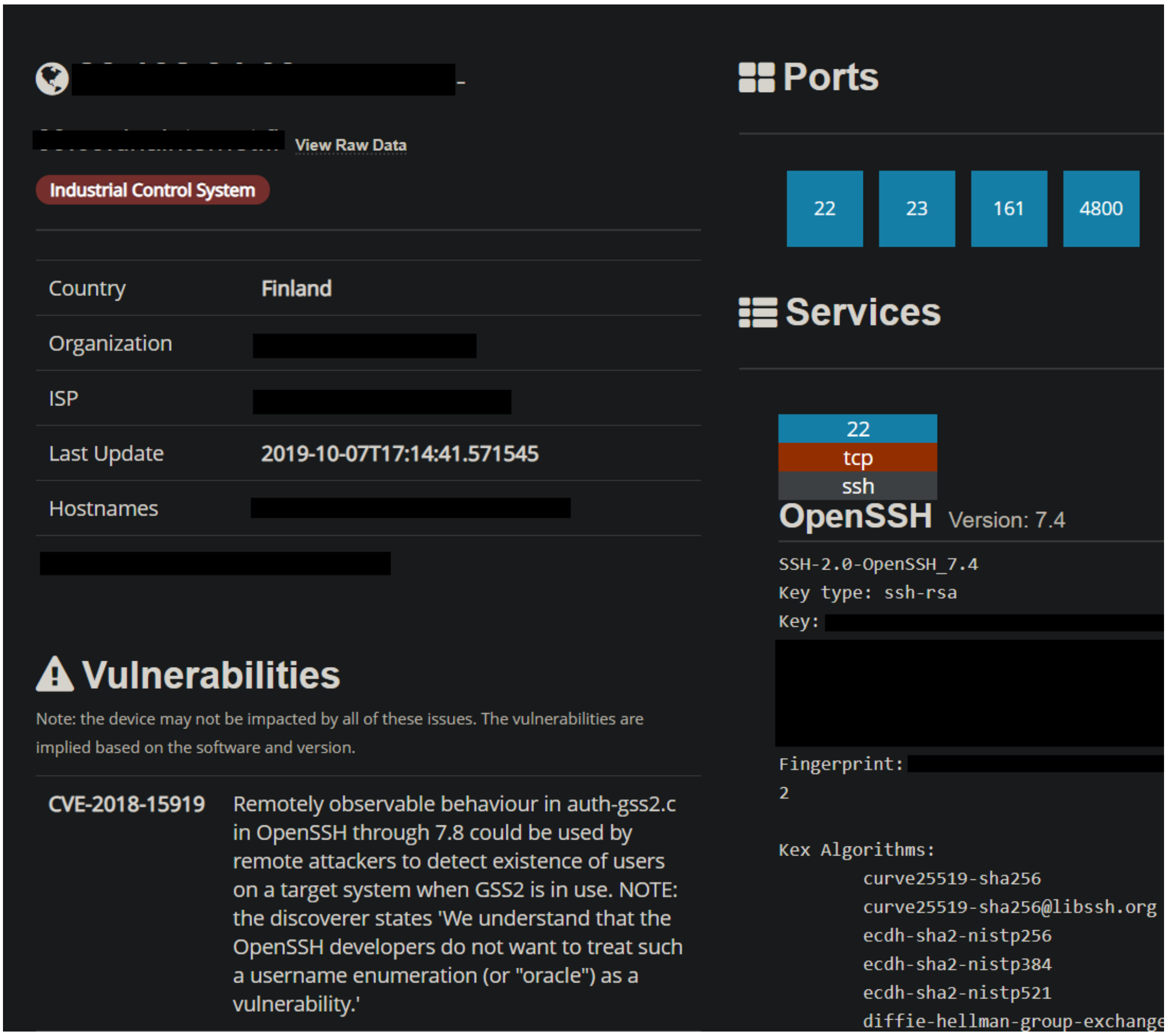
static.[redacted]

Hetzner Online GmbH

Added on 2019-10-06 21:59:44 GMT

Figure 10: Default password search in Finland (Shodan 2019)

Despite the potential threats and possibilities posed by Shodan, IoT device manufacturers and service providers have not been responsive concerning lax security, and most likely will not be until a global IoT hack with massive consequences occurs. An example scenario such an event could be a large-scale attack on industrial robots, ones that produce automobile or aircraft parts for example. In this case, human lives might be in danger without anyone realizing it. Figure 11 shows an example of a connected industrial system with possible vulnerabilities, located in Finland. This device was found using a straightforward search query and discovering said device took no longer than a minute.



[redacted] -

[redacted] View Raw Data

Industrial Control System

Country	Finland
Organization	[redacted]
ISP	[redacted]
Last Update	2019-10-07T17:14:41.571545
Hostnames	[redacted]

[redacted]

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2018-15919	Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'

Ports

22 23 161 4800

Services

22
tcp
ssh

OpenSSH Version: 7.4

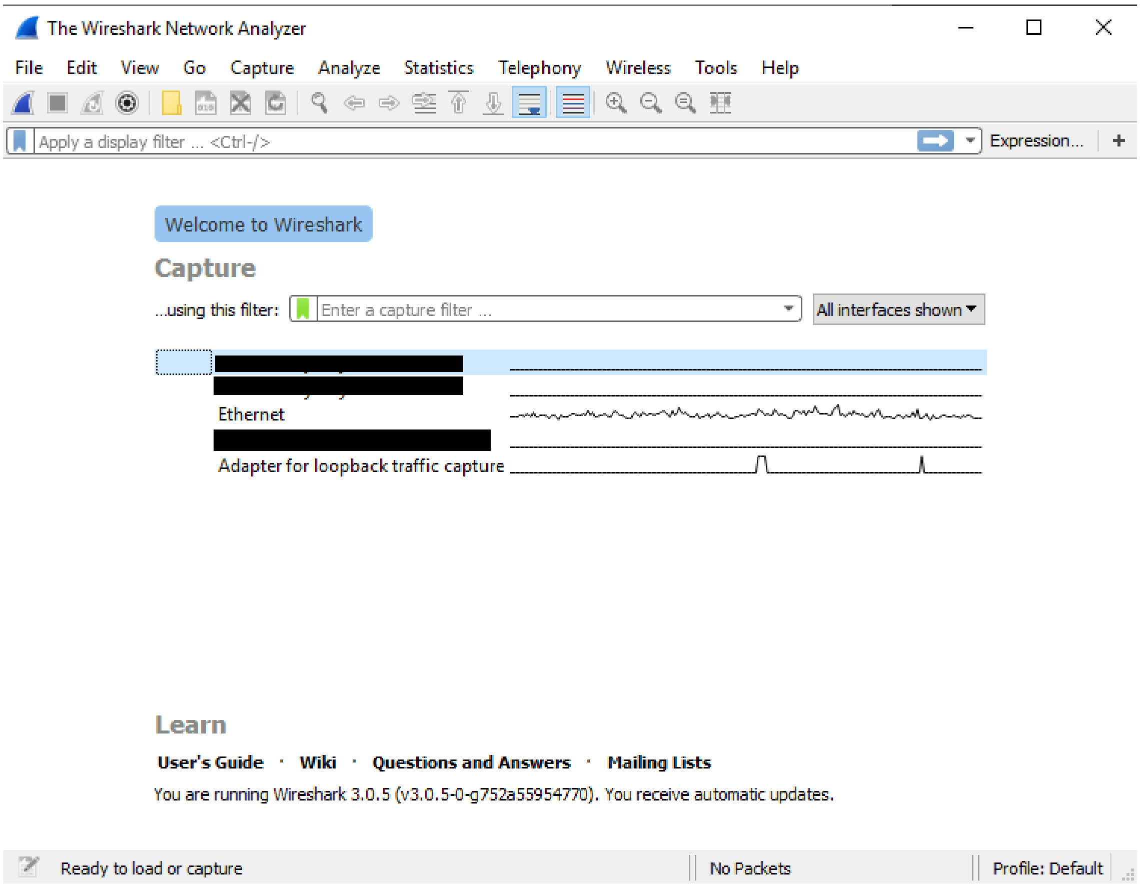
```
SSH-2.0-OpenSSH_7.4
Key type: ssh-rsa
Key: [redacted]
Fingerprint: [redacted]
2

Kex Algorithms:
        curve25519-sha256
        curve25519-sha256@libssh.org
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
        diffie-hellman-group-exchange
```

Figure 11: Potentially vulnerable industrial control system (Shodan 2019)

In Shodan, searches are done in a form such as “country: US”. By using this search query, for example, Shodan tries to discover every device open to the internet in the United States, which at the time of writing is over 182 million devices. Shodan also allows one to use search queries performed by others, as a template, which makes learning search functions easier for the user. Searching for routers that use the factory default login information is done by simply typing in “admin+1234”, which results in Shodan finding over 3400 such devices at the time of writing. (Shodan 2019).

4.2.3 Wireshark

Wireshark is an open-source software tool used for analyzing different network protocols. It is used to troubleshoot and analyze networks and can be used with IoT networks as well. In practice, Wireshark tracks network traffic for a particular port or protocol, with users then being able to view captured data via a GUI, or via the TTY-mode TShark utility. Figure 13 below shows the main view in Wireshark.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ...

All interfaces shown

[redacted]

Ethernet

[redacted]

Adapter for loopback traffic capture

Learn

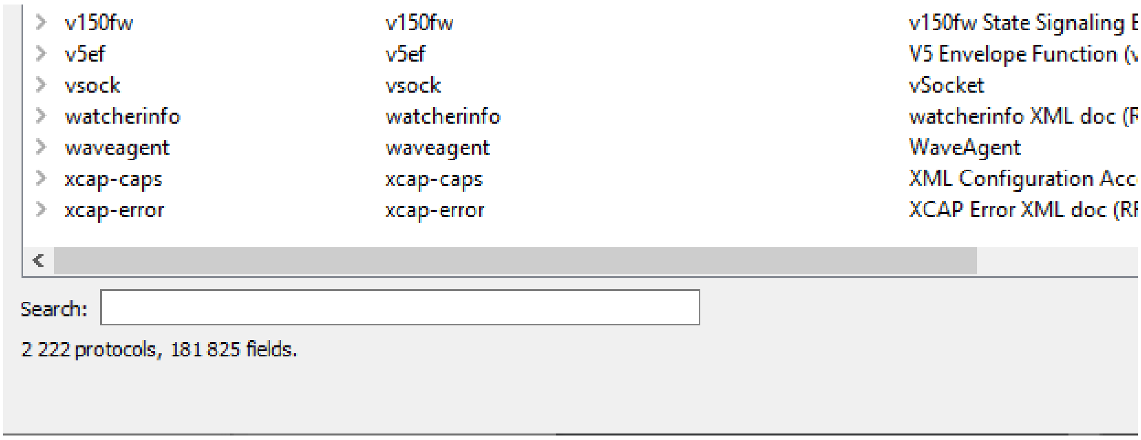
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.0.5 (v3.0.5-0-g752a55954770). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Figure 12: Wireshark main view (Wireshark 2019)

Wireshark can also decrypt many protocols used to protect wired and wireless networks, such as WEP, WPA/WPA2, IPSec, and even Kerberos. As of 2019, Wireshark supports over 2200 protocols in total (Wireshark 2019). Shown in Figure 14 is the bottom of a long list of protocols in Wireshark, with the total amount shown in the bottom left corner.



v150fw	v150fw	v150fw State Signaling E
v5ef	v5ef	V5 Envelope Function (v
vsock	vsock	vSocket
watcherinfo	watcherinfo	watcherinfo XML doc (R
waveagent	waveagent	WaveAgent
xcap-caps	xcap-caps	XML Configuration Acc
xcap-error	xcap-error	XCAP Error XML doc (RF

Search:

2 222 protocols, 181 825 fields.

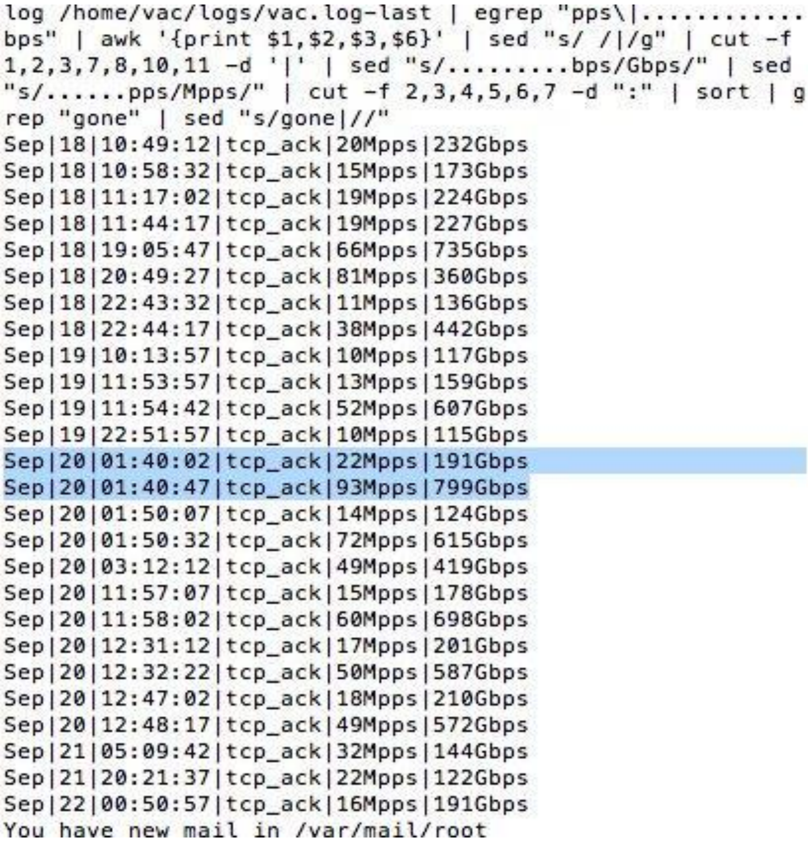
Figure 13: Wireshark protocols (Wireshark 2019)

5 Vulnerabilities and attacks

Manufacturers of IoT devices specifically designed for consumers are generally manufacturers of home appliances and do not always have an understanding of how the device security should be designed and/or implemented, which causes the device to be potentially exposed to various attacks from different directions of the network. This chapter provides some examples of vulnerabilities and attacks on IoT devices.

5.1 2016 Mirai botnet

Mirai is malware that infects smart devices that run on ARC processors, turning them into a network of remotely controlled bots, called a botnet, which are often used to launch DDoS attacks. In September 2016, the creators of Mirai launched a botnet DDoS attack against French host OVH, with simultaneous traffic totaling close to 1Tbps (Klaba 2016). Figure 17 shows the peak network traffic during the first attacks on OVH.



```
log /home/vac/logs/vac.log-last | egrep "pps\|............
bps" | awk '{print $1,$2,$3,$6}' | sed "s/ /|/g" | cut -f
1,2,3,7,8,10,11 -d '|' | sed "s/.........bps/Gbps/" | sed
"s/......pps/Mpps/" | cut -f 2,3,4,5,6,7 -d ":" | sort | g
rep "gone" | sed "s/gone|//"
Sep|18|10:49:12|tcp_ack|20Mpps|232Gbps
Sep|18|10:58:32|tcp_ack|15Mpps|173Gbps
Sep|18|11:17:02|tcp_ack|19Mpps|224Gbps
Sep|18|11:44:17|tcp_ack|19Mpps|227Gbps
Sep|18|19:05:47|tcp_ack|66Mpps|735Gbps
Sep|18|20:49:27|tcp_ack|81Mpps|360Gbps
Sep|18|22:43:32|tcp_ack|11Mpps|136Gbps
Sep|18|22:44:17|tcp_ack|38Mpps|442Gbps
Sep|19|10:13:57|tcp_ack|10Mpps|117Gbps
Sep|19|11:53:57|tcp_ack|13Mpps|159Gbps
Sep|19|11:54:42|tcp_ack|52Mpps|607Gbps
Sep|19|22:51:57|tcp_ack|10Mpps|115Gbps
Sep|20|01:40:02|tcp_ack|22Mpps|191Gbps
Sep|20|01:40:47|tcp_ack|93Mpps|799Gbps
Sep|20|01:50:07|tcp_ack|14Mpps|124Gbps
Sep|20|01:50:32|tcp_ack|72Mpps|615Gbps
Sep|20|03:12:12|tcp_ack|49Mpps|419Gbps
Sep|20|11:57:07|tcp_ack|15Mpps|178Gbps
Sep|20|11:58:02|tcp_ack|60Mpps|698Gbps
Sep|20|12:31:12|tcp_ack|17Mpps|201Gbps
Sep|20|12:32:22|tcp_ack|50Mpps|587Gbps
Sep|20|12:47:02|tcp_ack|18Mpps|210Gbps
Sep|20|12:48:17|tcp_ack|49Mpps|572Gbps
Sep|21|05:09:42|tcp_ack|32Mpps|144Gbps
Sep|21|20:21:37|tcp_ack|22Mpps|122Gbps
Sep|22|00:50:57|tcp_ack|16Mpps|191Gbps
You have new mail in /var/mail/root
```

Figure 14: September 2016 DDoS traffic against OVH (Klaba 2016)

Later that month, the code for Mirai was posted online by its creators, which is a technique that can give malware creators plausible deniability, as copycats tend to use code like this, which can lead to the waters being muddied on who used the code first. (CSO Online 2018).

Mirai can launch both network-level and HTTP flood attacks, and upon successful infection, it looks for other malware on that device and wipes it out, to claim the gadget as its own. By Design, Mirai avoids specific IP address ranges, including those owned by Hewlett-Packard, GE, and the U.S. Department of Defense. Mirai's code also contains some strings of Russian, inserted as a red herring by its creators to throw off the search for its origins. (CSO Online 2018).

Mirai has given birth to different variants based on its original code, such as Satori, Okiru, Masuta, and PureMasuta. These variants “improve” upon the original code, becoming more dangerous. PureMasuta, for example, can use the Home Network Administration Protocol bug that exists in D-Link devices. (The Register 2018).

5.2 2012 Trendnet webcam hack

In 2012, hackers posted live feeds to the web from nearly 700 webcams made by Trendnet. Trendnet marketed their SecurView cameras to have many different uses, such as baby monitoring and home security, but they had lax security features in that the software running in them allowed anyone who obtained the camera’s IP address to look through them and in some cases even listens. (TechNewsWorld 2013).

Later in 2012, after an official United States Federal Trade Commission inquiry, Trendnet patched the camera’s firmware, which should have never had security holes as it did. Trendnet displayed negligence toward the big picture of security and IoT in general by allowing their devices to roll out with such vulnerabilities. Kevin O’Brien, and enterprise solution architect at CloudLock states "Don't over connect your systems, don't trust a locally compromised or accessible device, and do subject your code and hardware to third-party penetration testing, both in black box and white box variants”, which is good advice for IoT providers, organizations, and some more tech-savvy consumers. A simple penetration test by Trendnet during the development process of their SecurView cameras could have prevented this incident. (TechNewsWorld 2013).

5.3 Lack of compliance

One of the most significant issues in IoT devices is not a vulnerability in itself, but rather an issue which causes them - a lack of compliance in manufacturing. According to Intellectsoft (2019), new IoT devices come out almost daily, all with undiscovered vulnerabilities. Manufacturers that are starting to add Internet connectivity to their devices do not tend to have a security-first mindset during the design process of their product due to a lack of time, resources, caring, or a combination of the three.

Hardware issues, unsecured update mechanisms, unpatched software, and embedded systems, and weak default passwords are all vulnerabilities that stem from manufacturers not investing enough into security. As long as there is an absence of common IoT security standards that manufacturers must adhere to, they will keep shipping out devices with weak security. (Intellectsoft 2019).

6 Consumer security solutions

Consumers and organizations are currently being offered a wide range of IoT device security enhancing devices. Many security companies have recently gotten involved in improving IoT‘s overall security by beginning to develop devices to enhance both home and organizational IoT security. In this chapter, I present 2 consumer options for protecting a home network when IoT devices are involved.

6.1 Bitdefender BOX

One option for consumers to improve their home network and IoT device security is the Bitdefender Box made by respected cybersecurity and antivirus software provider Bitdefender. The Bitdefender BOX protects the home network in different ways, by filtering suspicious URLs based on the manufacturer's database. It also scans every device on the network for potential vulnerabilities every three days. During this scan, it checks for firmware updates, password strengths, and other weaknesses. The device comes with access to Bitdefender’s Total Security software and their Private Line VPN service, which lets users create a secure wired or wireless connection from outside their home. (Bitdefender 2019).

The device can be used either with an existing standalone Wi-Fi router, as a Wi-Fi router on its own, or with an ISP-provided gateway router. Bitdefender does state that the BOX cannot compete with high-end standalone routers, and it is not marketed to be one. According to Tom’s Guide (2018), the slight hit in network speed when using the BOX along with a high-end router is worth it, though, as the added security features that the device brings do make the dip in data rate worth it (Tom’s Guide 2018). Figure 15 shows the interface of Bitdefender’s mobile application.

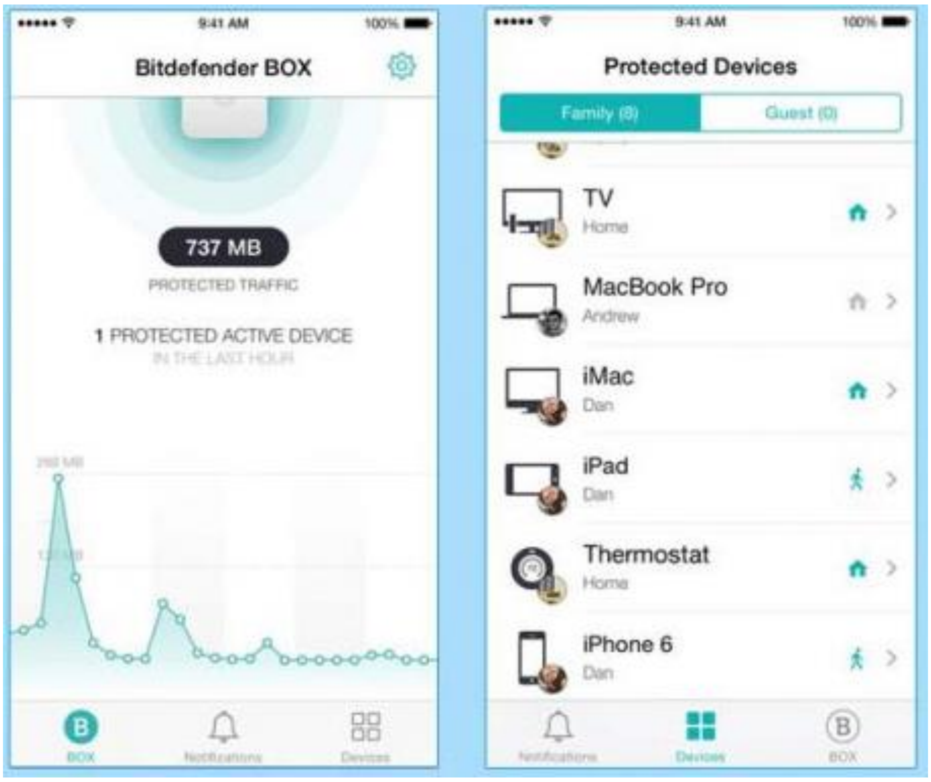


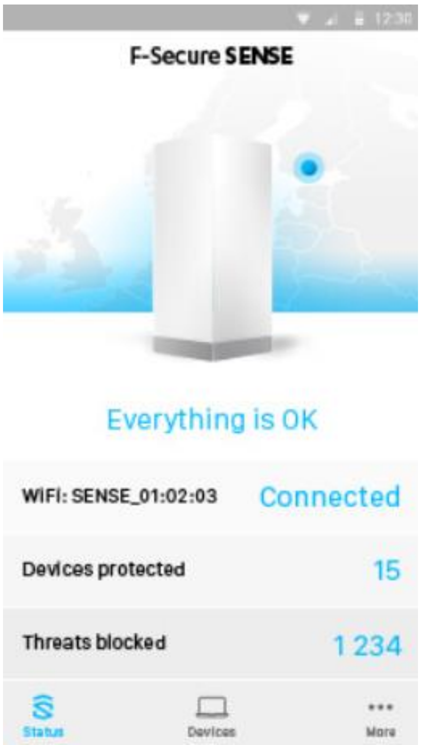
Figure 15: Bitdefender BOX mobile interface (Tom’s Guide 2016)

The Bitdefender BOX starts at $179.99, which includes a 1-year subscription to Bitdefender Total Security, and the device itself along with an install & setup service. (Bitdefender 2019).

6.2 F-Secure Sense

Finnish cybersecurity company F-Secure provides security products for both consumers and businesses, which include antivirus software, a VPN, and the Sense security router. The company also has enterprise-specific security software capable of protecting terminals and network traffic. (F-Secure 2019) Mikko Hyppönen, F-Secure’s Chief Research Officer, has been an active speaker in IoT security in recent years, pushing people and organizations to secure their IoT devices and networks. (The Register 2017, 2).

“Sense” is F-Secure's hardware-based security solution for home use. The Sense package includes hardware, software, and mobile software. Unlike the Bitdefender BOX, Sense cannot be used without a separate router. It and the existing router form a new secure Wi-Fi network to connect the user’s home devices (including IoT ones) to, which monitors communications in F-Secure's cloud service. F-Secure's cloud service is called Secure Cloud, and it collects data about unknown applications, websites, and malicious applications, which is anonymously sent to F-Secure for analysis. F-Secure then uses the data to improve customers’ protection against the latest threats. Sense is monitored using a mobile app, pictured in Figure 16, which displays all pertinent information to the user, such as connected devices, updates, and blocked threats. (F-Secure 2019,2).



Everything is OK

WIFI: SENSE_01:02:03	Connected
Devices protected	15
Threats blocked	1 234

Figure 16: Sense mobile app interface (F-Secure 2019, 3)

The prices for the device start at $179.99, which includes the router itself, along with a subscription to F-Secure’s TOTAL cybersecurity suite. (F-Secure 2019, 3) Some reviewers have stated that the initial cost is expensive (CNET 2017), but it warrants the added security. Based on the information and reviews available, security solutions such as the BOX and the Sense are worthwhile options for consumers to improve their home network and IoT device security, at a reasonable price.

7 Conclusion

The field of IoT is a continually changing one. New types of devices are being created every day, and along with them, new threats and vulnerabilities. There is no simple solution to security in IoT, so device manufacturers and service providers must always be aware of new security threats. The field of IoT covers such a large number of devices and applications that it is currently impossible to provide a comprehensive solution. Because technology is continually moving forward, security must keep up. The regulatory landscape around IoT is a hazy one at its best, but new and improved regulations are being drafted and put into action, which will help with device security, and thus, with end-user satisfaction and peace of mind in the long run. Cybersecurity is forever a constant source of rivalry between attackers and defenders. When selecting equipment, systems, and technologies to use, one should address the vulnerabilities that are most easily repaired and exploited.

For consumers, there exists a lot of information online on IoT technology and the benefits it can bring to the household and the users' daily life. Security suites and solutions exist for consumers at a reasonable price, and one should think about acquiring one for the home if they have IoT devices.

Organizations and consumers alike will all benefit immensely from a secure IoT, and the future is looking bright for the technology and its millions of potential applications. However, one should remember that only thinking of the benefits of IoT without seeing security as a crucial component is a bad idea. Listed below are some best practices for IoT security based on my findings, for consumers and organizations.

- Consumers should research the features, especially security ones, of the device or security suite that they are planning to purchase, while organizations should be proactive with security, and consider the possible risks that IoT devices introduce into their corporate ecosystem, while also educating employees on these risks.

- Unneeded functionality, such as microphones, cameras, or even connectivity itself in some cases, should be turned off, especially in corporate environments with sensitive information around.

- Careful research of the backend security characteristics and controlling applications should be conducted, and for both enterprises and consumers, devices that rely on apps or services that maintain poor security or privacy should not be used. Consumers should look up reviews from trusted tech reviewers or security experts on whether to make their purchase decision.

- Physical access should never allow intrusions, such as via a factory reset or an easily accessible hardware port. Hardware ports, especially on the server-side of the network, should always be kept behind lock and key.
- Monitoring the lifecycle of devices in an IoT network is always a good idea. Devices should be removed from service once they are no longer secure or updateable.

8 Reflection

With completing this thesis, I was able to benefit from a variety of new information that I discovered and presented, as well as refresh my memory on things that I already knew. This includes things such as best practices for information security and cybersecurity, but also academic writing and information gathering.

A big hurdle for me was the research methods of my work. I am a very impulsive writer, and I wanted to immediately start researching and writing about IoTs while ignoring possible research methods and the outline of my paper, which did not help in the long run. Also, being a procrastinator is not helpful when dealing with a document that requires that the reader is presented with some background on the research methods and the work itself. Despite these hurdles, I learned many new things about the way the world is connected right now and where it may be headed from here, which will surely benefit me in my work career or when possibly pursuing a higher degree. All in all, this thesis was a challenging yet rewarding project and a learning process.

References

Printed sources

Bowen, G. 2009. Document Analysis as a Qualitative Research Method. Victoria: RMIT

Gilchrist, A. 2017. IoT Security Issues. Berlin: Walter de Gruyte

Mack et al., 2005. Qualitative Research Methods: A Data Collector's Field Guide. Research Triangle: USAID

Matherly, J. 2016. Complete Guide to Shodan. Victoria: Lean Publishing

Whitman, E., Mattford, H. 2012. Principles of Information Security. Boston: Course Technology

Electronic sources

Arm 2019. Internet of Things Applications. Viitattu 24.6.2019
https://www.arm.com/solutions/iot/iot-applications

APQC 2016. Supply Chain 2016 Outlook: Survey Summary Report. Viitattu 7.9.2019.
https://www.apqc.org/resource-library/resource-listing/supply-chain-2016-outlook-survey-summary-report

Bhat, O., Bhat, S. & Gokhale, P 2017. Implementation of IoT in Smart Homes. Viitattu 2.8.2019 https://www.researchgate.net/publication/330114746_Implementation_of_IoT_in_Smart_Homes

Bitdefender 2019. Bitdefender BOX. Viitattu 20.10.2019
https://www.bitdefender.com/box/

Cisco 2011. The Internet of Things: How the Next Evolution of the Internet
Is Changing Everything. Viitattu 29.10.2019
https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Cloudflare 2019. What is penetration testing? Viitattu 10.8.2019
https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/

CSO Online 2018. The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet. Viitattu 15.10.2019
https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Domb, S. 2019. Smart Home Systems Based on the Internet of Things. Viitattu 3.8.2019
https://www.intechopen.com/online-first/smart-home-systems-based-on-internet-of-things

Ericsson 2016. Wearable technology and the IoT. Viitattu 8.8.2019
https://www.ericsson.com/en/trends-and-insights/consumerlab/consumer-insights/reports/wearable-technology-and-the-internet-of-things

Forbes 2014. A Simple Explanation Of 'The Internet Of Things.' Viitattu 22.6.2019 https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/

F-Secure 2019. F-Secure products for home. Viitattu 11.10.2019 https://www.f-secure.com/en/home/products

F-Secure 2019, 2. What is Security Cloud? Viitattu 11.10.2019 https://community.f-secure.com/t5/F-Secure-SAFE/What-is-Security-Cloud/ta-p/77895

F-Secure 2019,3. What is F-Secure Sense? Viitattu 11.10.2019 https://www.f-secure.com/en/web/home_global/Sense

Gartner 2016. Technologies Underpin the Hype Cycle for the Internet of Things, 2016. Viitattu 3.9.2019. https://www.gartner.com/smarterwithgartner/7-technologies-underpin-the-hype-cycle-for-the-internet-of-things-2016/

GE Digital 2019, 1. Everything you need to know about the Industrial Internet of Things. Viitattu 1.9.2019 https://www.ge.com/digital/blog/everything-you-need-know-about-industrial-internet-things

GE Digital 2019, 2. GE Advances Digital Leadership with Launch of $1.2 Billion Industrial IoT Software Company. Viitattu 4.9.2019. https://www.ge.com/digital/blog/ge-advances-digital-leadership-launch-12-billion-industrial-iot-software-company

IBM 2015. IBM Point of view: Internet of Things security. Viitattu 2.9.2019 https://www.ibm.com/downloads/cas/7DGG9VBO

InfoSec Institute 2018. Pentester’s Guide to IoT Penetration Testing. Viitattu 21.8.2019 https://resources.infosecinstitute.com/pentesters-guide-to-iot-penetration-testing/

Intellectsoft 2019. Top 10 Biggest IoT Security Issues Viitattu 23.10.2019 https://www.intellectsoft.net/blog/biggest-iot-security-issues/

IoT For All 2019. Where Do Wearables Fit into the Internet of Things? Viitattu 7.8.2019 https://www.iotforall.com/where-wearables-fit-in-iot/

IoT Security Foundation 2018. IoT Cybersecurity: Regulation Ready. Viitattu 20.6.2019 https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Cybersecurity-Regulation-Ready-White-Paper-Concise-Version.pdf

i-SCOOP 2018. The Industrial Internet of Things (IIoT): the business guide to Industrial IoT. Viitattu 10.9.2019 https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/

Octave Klaba 2016. Tweet on September 2016 DDoS attacks. Viitattu 13.10.2019 https://twitter.com/olesovhcom/status/778830571677978624

Norton 2019. 12 tips to help you secure your smart home and IoT devices. Viitattu 25.8.2019 https://us.norton.com/internetsecurity-iot-smart-home-security-core.html

O’Leary, Z 2018. 10 Steps to Demystify the Research Process. Viitattu 15.11.2019 https://www.methodspace.com/10-steps-demystify-research-process

Rapid7 2017. Metasploit's RF Transceiver Capabilities. Viitattu 10.8.2019 https://blog.rapid7.com/2017/03/21/metasploits-rf-transceiver-capabilities/

Shodan 2019. Shodan home page. Viitattu 7.10.2019.
https://www.shodan.io/home

Sigfox 2019. The New IoT-Powered Supply Chain: How Smart Logistics Tracking is Creating a Leaner, More Agile Global Economy. Viitattu 25.6.2019
https://www.sigfox.com/en/new-iot-powered-supply-chain-how-smart-logistics-tracking-creating-leaner-more-agile-global-economy

Security Alliance 2016. Encouraging Customers to Upgrade to Alarm.com. Viitattu 8.9.2019
https://www.securityalliance.us/news/encouraging-customers-to-upgrade-to-alarm-com/

TechNewsWorld 2013. Webcam Maker Takes FTC's Heat for Internet-of-Things Security Failure. Viitattu 28.10.2019. https://www.technewsworld.com/story/78891.html

The Register 2017. Metasploit upgraded to sniff out IoT weak spots in corporate networks. Viitattu 20.8.2019. https://www.theregister.co.uk/2017/03/22/metasploit_iot_upgrade/

The Register 2017, 2. F-Secure's Mikko Hypponen on IoT: If it uses electricity, it will go online. Viitattu 9.10.2019
https://www.theregister.co.uk/2017/06/21/fsecure_mikko_hypponen_Sense_interview/

The Register 2018. Fresh botnet recruiting routers with weak credentials. Viitattu 13.10.2019
https://www.theregister.co.uk/2018/01/24/fresh_botnet_recruiting_routers_with_weak_credentials/

Tom’s Guide 2016. Bitdefender Box Review: Wi-Fi Security (with Free VPN and Antivirus). Viitattu 22.10.2019
https://www.tomsguide.com/us/bitdefender-box-2016,review-5054.html

Tom’s Guide 2018. Bitdefender Box Review: Flexible Protection. Viitattu 22.10.2019
https://www.tomsguide.com/us/bitdefender-box,review-3766.html

T-Systems 2019. From concept to reality. Viitattu 17.8.2019.
https://www.t-systems.com/gb/en/newsroom/perspectives/internet-of-things/series-internet-of-things/autonomus-drive-863804

Wireshark 2019. About Wireshark. Viitattu 8.10.2019
https://www.wireshark.org/

Figures