IoT Security

Lennart Heim

Abstract

The Internet of Things (IoT) describes the expansion of the Internet and embedded technologies to everyday devices. It has been on the rise for the last years and it will certainly continue – Ericsson, for example, forecasts about 29 billion connected devices by 2022. This rapid growth changes the network landscape dramatically and recent studies reveal an increased threat by vulnerable and malware infected IoT devices.

This report discusses the introduced challenges of IoT devices and outlines common security risks. Furthermore reasons for the increased vulnerability and their consequences for the network and the privacy of users will presented.

As an example for a security incident, the example of the botnet Mirai will be presented. Mirai was one of the biggest and most powerful DDoS attacks ever seen. Technically it was a simple incident, nonetheless it ended up rendering big parts of the Internet inaccessible.

To overcome the security issues introduced by the IoT, technical and policy mitigations will be presented. Technical mitigations in general focus on good security practices and well known practices which have been known for years. However, due to technical reasons, and market incentives, those practices were often not applied to IoT products. As a response, policies for manufactures were proposed by multiple security experts, which might help to decrease the threat of IoT devices in the networked world. Inspired by already known policies from other markets, several proposals to increase the security of the network and safeguard the privacy of the users will be presented.

January 28, 2020

CONTENTS

I. Introduction

The Internet of Things (IoT) is the expansion of the Internet and embedded technologies to everyday devices. Ericsson forecasts about 29 billion connected devices by 2022, given the immense interest in IoT devices and their cheap costs. Furthermore the revenue of the IoT market is rapidly growing, as more connected devices are released and make their way into the consumer markets and their homes. It is a trend with no end in sight, as the application field is also expanding [1].

IoT devices are by definition heterogeneous and cover multiple applications and fields, such as environment sensing, home assistants, assets tracking, security and more. The essential part of an IoT device is the interaction with the physical world, and the interconnection to a network – either local, or to the Internet. The growth in IoT products has been immense, and will continue growing – it is a disruptive technology with the potential for impact.

Nonetheless, according to various security experts the introduction of the IoT has changed the network landscape and has increased the threat introduced by vulnerable and malware infected IoT devices. This rapid growth changes the network landscape dramatically and recent studies reveal an increased threat by vulnerable and malware infected IoT devices [2].

Compared to traditional information technology devices, IoT devices have a different impact on cybersecurity, and additionaly on the privacy of the users – ubiquitous features have invaded the privacy. Consequently the increased security threat is a concern for the network, but also for the privacy of the users.

In addition the market growth around the IoT resulted in poorly manufactured devices with many security flaws, as the time to market and cheap prices are essential. Due to the enormous pace and the need of cheap development costs, the security of devices is often of low priority [3].

This seminar report will first outline the architecture of the IoT, but also of IoT devices. Based on the architecture multiple attack vectors will be covered. In the following section the challenges and constraints of IoT devices will be described, as they are the important factors. Based on the security attacks and vectors, the consequences will be presented – consequences for the network, but also for the privacy of the user. Furthermore I will outline the example of the botnet Mirai – a well known security issue in the year 2016. Lastly, I will discuss mitigations to overcome the increased security risk by the IoT – by technical but also policy mitigations.

II. Security in the IoT

The term Internet of Things (IoT) has no strict definition – usually it describes the expansion of the Internet and embedded technologies to everyday devices. Given the heterogeneity of IoT devices there is not one IoT device architecture, or one layer which contains all the security issues – IoT is a lose term, and describing common features is complex. The following paragraphs provide a description of a general architecture of IoT devices and will then continue to focus on security issues at the individual components.

The common model for security goals is: *confidentiality*, *integrity*, and *availability*. Confidentiality describes the protection of the data and the ability for a safe access. Integrity confirms that the data is real and accurate, but also the protection against modification by unauthorized users. Lastly, availability describes the ability to access the data by only authorized users at all time. This is commonly described as the CIA triad [4].

A. Internet of Things Architecture

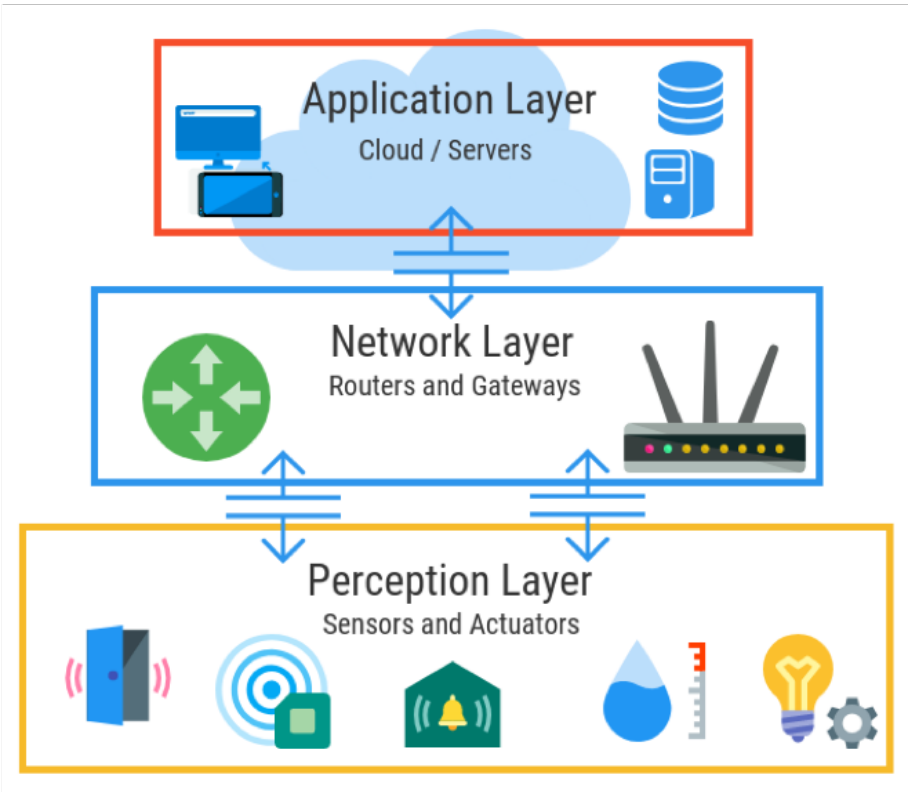

Fig. 1. IoT Architecture (taken from [5])

Figure 1 presents a common model for the architecture of the IoT. The model is divided within 3 layers: application, network and perception. The following subsections will present each layer.

1) Perception layer: IoT devices are usually devices which monitor the physical world. Therefore the perception layer gathers information using all kinds of different sensors, also multiple sensors on the same device which then accumulates the data. Typical examples are temperature sensors, humidity sensors, microphones, cameras etc. [5], [6].

2) Network layer: The network layer is the link between the perception layer and application layer. It enables the (secure) transmission of collected data to the application. Moreover, remote access to the physical devices is also often provided by the network layer – whereas traditional device can only be accessed physically or locally. Typically the network layer consists of traditional protocols like TCP/IP, and uses more novel protocols for the physical transmission – often wireless. In the wireless domain the usage of a IEEE 802.11 standard is common, but also special designed wireless protocols for the IoT domain, e.g. LoRa [5], [6].

3) Application layer: The final layer is the application layer. The application layer is the interaction layer for the users where all the gathered data will be processed and presented to the user. Further processing and analysis of the data is usually conducted at this layer – like notifications and warnings due to sensed events from the IoT device. This layer often resides in a centralized cloud at the manufacture, or a hosted service.

However, sometimes the processing and presentation of the data can also be provided locally by the device if the capabilities allow so. Typically the device then runs an embedded operating system (OS), for example a Linux distribution [5], [6].

B. Internet of Things Architecture Security

All of the presented layers play a crucial role in the security of the IoT. The following subsections will present their security risks and name examples of possible attack vectors.

1) Perception layer security: The most common security issue in the perception layer is the detection of an abnormal sensor node. Sensor nodes can deliver faulty data due to physical attacks, but also due to security issues. Therefore the detection of abnormal sensor states is an important feature, as faulty data can have tragic consequences when the device is monitoring critical infrastructure [5], [6].

Furthermore attacks on correctly working sensors are also possible using stealth mechanism – an example for this are, so called, Dolphin Attacks where without the knowledge or ability from the users to hear, the sensors of the IoT device receives a command [7].

2) Network layer security: In general an end-to-end encrypted network connection is of interest. However, the encryption has to happen on multiple layers and has be implemented correctly. Therefore the network layer security is similar to the ones of conventional IT equipment and faces the same security risks, like illegal network access, DoS attacks, man-in-the-middle attacks, exploit attacks and more [3], [6]. In addition the current network landscape is still based on the perspective of persons and is not optimized for machine-to-machine communication [6].

Nonetheless, the IoT introduced multiple new novel wireless network protocols. The interest in less computing intense, and more energy efficient networking resulted in multiple new wireless protocols, like LoRa, or ZigBee. The introduction of new protocols always comes at an increased risks, as they are not as reliable and well tested, as traditional ones, like the IEEE 802.11 family [5], [6].

3) Application layer security: The wide variety of IoT applications results in multiple security considerations on the application layer. Authentication methods at the application layer are always the biggest security concern. The authentication needs to be secure technically, but also enforce strong passwords policies – otherwise a full access to the device is possible. This is important to enable data protection and block unauthorized access. Furthermore the integrity of data – that no manipulation has taken place – has to be ensured [5], [6].

Modern IoT devices usually contain embedded computer systems which are running complex software – often a Linux for embedded devices. Therefore they face the same security

risks as conventional computers, however often they lack the defense mechanisms due to limited hardware. An example for this is the remote code execution via shell access via `ssh` or `telnet`, which will be presented in the example of Mirai in Section III.

Overall, the IoT describes a wide diversity of devices involving all the layers of modern computer systems. Given this heterogeneity of devices many security challenges have to be considered when developing an IoT device, but also an IoT service. New security issues arise, but also existing ones become more serve.

C. Challenges

In this subsection the reasons for the increased vulnerability and threats for the IoT will be discussed. Furthermore, the differences to conventional IT devices explains why existing security issues have become more critical with the introduction of the IoT.

1) Communication: A key feature of IoT device is the communication with their environment – to other IoT devices, an application server, or the user. Therefore IoT devices are usually connected to the Internet using wireless technologies. Conventional embedded devices which reside in a wide variety of devices were not connected to the Internet and acted as a standalone device – the IoT changed this. Introducing the networking stack to devices comes with increased hardware and software requirements, but most importantly it allows for the device to communicate with the outside world – and the outside world with the device [2], [8]–[10].

2) Heterogeneity: The IoT is just a collection term for a wide diversity of devices, it is hard to summarize or implement security features which apply to all IoT devices.

IoT devices have a wide variety on application areas and are therefore by definition diverse. The security requirements do therefore also differ for each application area. While the industry asks for high reliability and secure devices, consumers are probably more interested in aesthetics and functionality.

Monitoring or managing the IoT devices usually requires new techniques, as they cannot be managed like conventional IT devices. Therefore, there is no one solution-fits-it-all on software and hardware site [2], [8]–[10].

3) Scale: The idea of embedding computers into everyday devices results in a massive scale of IoT devices. The Internet has never seen more online devices than now – and the trend is continuing. This development asks for novel ideas within the network and communication sector, as the increase in the devices challenges the current network infrastructure. Already known attacks on networks like the creation of botnets, or distributed denial-of-service (DDoS) attacks become way more powerful and increase the threat on the Internet immensely. A single security flaw within an IoT product can cause personal data leaks or DDoS attacks of thousands of devices.

Consequently, the availability and effectiveness of defense mechanism for attacks on the network are different for IoT devices than for conventional IT devices [2], [8]–[10]. In Section III, the Mirai botnet will be presented which made use of the huge number of IoT devices.

4) Hardware constraints: Per definition IoT devices are small embedded devices which usually run on limited hardware to reduce costs and decrease their physical footprint. The usage of embedded microprocessor with limited capabilities introduces new engineering challenges. Compared to traditional computers, embedded devices usually run a microcontroller with limited computing capabilities and reduced memory. These hardware constraints therefore

ask for new and more efficient cryptography, as cryptography is memory and computing intense.

Furthermore most systems do not use an operating systems as a host – the developed software is running natively on the device. Features of operating systems, which are often security features, are missing and the device is more vulnerable. Third party software cannot be deployed on the device, e.g. anti-virus software [6], [9].

5) Energy efficiency: IoT devices are often battery powered and/or running around the clock, this asks for an efficient usage of energy. Implementing encryption algorithms always increases the computing load on the device and therefore increases the energy usage, especially as cryptography involves computing intense algorithms. Often developers optimized the energy usage, by using less secure algorithms, or non-secure at all.

Summarized, cryptography and authentication always raises the workload on the embedded devices and therefore increases the energy usage. Often those are the first feature which developers neglect, as most of the key features which customers care about, do not rely on good security [6], [9].

D. External drivers

In the previous subsection the technical reasons for missing security or faulty implemented security algorithms were outlined. However, the given technical challenges are amplified by external drivers – for instance financial incentives, or consumer priorities.

The market around IoT has always been described as one of the most innovative and fastest growing market. IoT devices were presented to solve a wide variety of problems which increased the consumer but also industry (Industry 4.0) demand – an IoT hype was created. This hype was the result of the convergence of cloud computing, mobile computing, embedded systems, big data, low-price hardware and technological progress [11]. As the market for IoT devices is widely unregulated, compared to traditional markets like automotive, or groceries, a short time to market was possible and essential. Manufactures have the motivation to be the first one on the market who is offering an IoT device within this branch. Nonetheless, this decreased development time comes at the cost of security. Implementing security does increase the cost and development time, especially within novel fields.

The second important factor is the consumer. Consumers have an increased demand for IoT device and are buying them in abundance. Some people are not even aware of how many IoT devices they are already using [11]. Taking the interest in multiple applications of IoT devices, or sometimes even multiple of the same IoT device, into considerations, results in an interest in cheap devices. However, cheap devices often lack good security, due to the need of low development costs.

Another driving factor is the missing knowledge on the consumers side. Consumers are not aware of the privacy problems introduced with the IoT and often lack basic knowledge about IT security. Therefore the security of an IoT devices has a low priority, or no priority when buying an IoT device [6], [12].

Taking all things into considerations, we have multiple pull factors in favor of manufacturing, selling and buying insecure IoT devices. Those are just some of the external drivers which resulted in hundreds of thousands, or up to millions of IoT device in the Internet which lack basic good security practices.

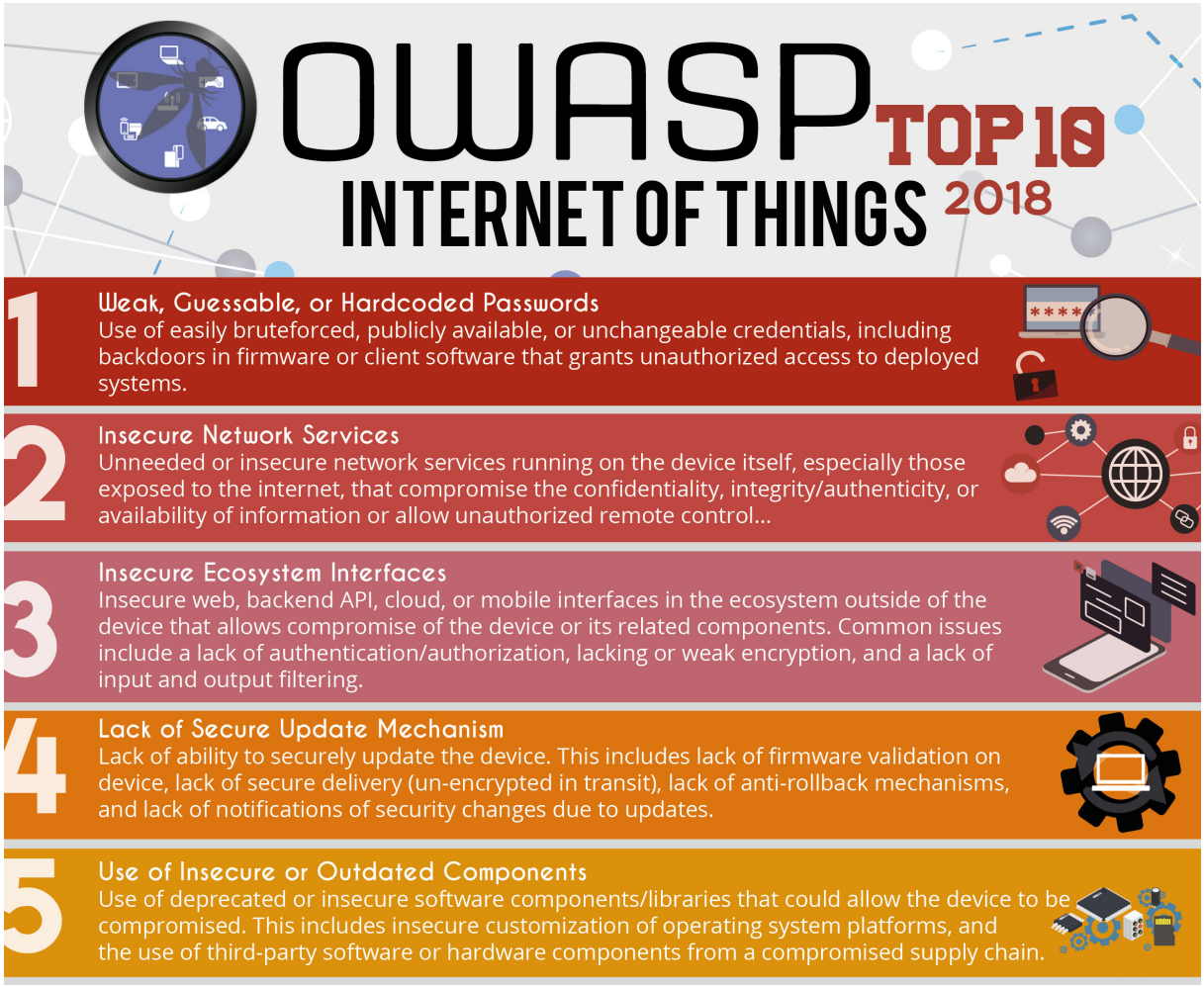

Fig. 2. OWASP Top 5 IoT Security Risks (taken from [13])

E. Most common security risks

The Open Web Application Security Project (OWASP)'s IoT project wants to help developers, manufactures and consumers to create better decisions regarding the IoT. The project was started in 2014 and releases irregularly a Top 10 list of things to avoid when *building, deploying, or managing IoT sytems* [13]. To summarize previously outlined risks, the OWASP Top 5 will be presented and discussed.

1) Weak, guessable or hard-coded passwords: The usage of weak passwords is one of the most common and worst security issues. Using weak, guessable or hard-coded passwords allow attacks to get unauthorized access to the system, which then often allows full access and remote code execution. Once holding these rights, there are no limits set - reflashing with malicious firmware, redirecting the network traffic, and more. This access is usually remotely and without restrictions [6], [8], [13].

2) Insecure network services: IoT devices usually offer network services to allow the communication with other IoT devices. However, often network services are enabled by default and not secured by authentication. Those network services often also enable some control of the IoT device – in critical cases also full access and code execution [6], [8], [13].

3) Insecure ecosystems interfaces: Compared to the previous security risks, the ecosystem interface is the interface usually at the application layer outside of the IoT device, often

hosted on external cloud services. Access to the ecosystem allows access to the data and often control to the device – all of it remotely. Subsequently, the security of the cloud service plays a crucial role [13].

4) Lack of secure update mechanism: The need of update mechanism is a critical feature for IoT devices, especially in the future, as presented in Section IV-A4. However, this update mechanism needs to be secured, to only allow updates of validated firmware and not malicious firmware injected by attackers [8], [13], [14].

5) Use of insecure or outdated components: Developers often rely on already existing libraries which are then used to implemented common function within their device. However, often outdated libraries, or insecure libraries are used. Those security risks are usually public knowledge and can then be used by malicious actors to compromise the device, the traffic, or the application [12], [13].

F. Consequences

The consequences of vulnerable IoT devices are immense – for the individual, but also for the Internet itself.

IoT is a mixture of diverse networked embedded devices, therefore it has the same security concerns, as sensor networks, or mobile communication networks and the Internet itself. However, due to the feature of monitoring physical worlds, it also introduced a privacy problem [6]. Likewise to traditional computer systems, security issues allow access to various kinds of information. In IoT devices however this information is from a wide variety of sensors which often monitor private spaces, but also critical infrastructure. As a result a major consequence of security issues is the privacy intrusion. Malicious actors can collect personal information or monitor users – from video feeds of cameras to the lighting within the living room, often without the awareness of the user. Additionally an aggregation and analysis of the data can result in a detailed analysis of the physical world, including their users and their habits [9], [15].

Furthermore, due to the scale and heterogeneity of the IoT, the network landscape has changed and experiences some increased risk. Insecure IoT devices can be compromised by malicious actors and become part of a botnet. This risk is of special interest to the IoT, as the threat by botnets does not only scale with the number of enslaved devices, but also with the geographical diversity of the devices. Overall this introduced new types and new scale of network attacks which have not been seen before – and the number of IoT devices is still growing [16], [17].

The following section will present the Mirai botnet, an example for one the biggest botnets ever seen, which is a result of IoT devices lacking basic security features.

III. Example: Mirai botnet

Mirai is a malicious software (malware) which was first discovered in 2016 during one of the largest and most disruptive DDoS attacks [18]. The translation of the Japanese term Mirai is *Future* – which it indeed highlighted in 2016, the future of network attacks by IoT devices. This malware turns IoT devices into remotely controlled bots and makes them part of a botnet[1]. Multiple botnets, the results of Mirai, were used for DDoS attacks which rendered big parts of the Internet inaccessible at certain time points [17].

The technical details of a DDoS attack are not of importance for this report. The significant factors are that a DDoS attacks get more powerful with bigger scale (more enslaved devices) and more geographical distribution (to not allow IP blacklisting based on their geographic location). Two well known features of the IoT – more scale and more distribution.

A. Mirai Timeline

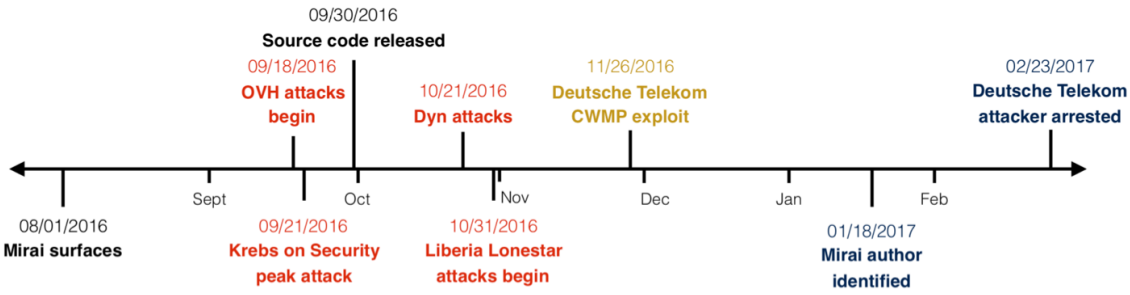

Fig. 3. Timeline of Mirai (taken from [18])

Mirai was first identified in August of 2016. At this point it already had enslaved $65,000$ IoT devices at the end of its first day.

In the following month, September 2016, a DDoS attack on OVH[2] was identified. This attack was first classified as a political motivated attacked, as OVH was hosting Wikileaks[3]. Brian Krebs, a well known security researcher, covered this incident on his blog and conducted research on the technical details. Shortly after publishing his findings, his blog was also attacked by major DDoS attacks [19].

The peak DDoS attack was seen in October 2016. The domain name server (DNS) hoster Dyn was attacked by Mirai and suffered enormous outages which lasted around a single day. Dyn was providing service for multiple popular companies like Twitter, Spotify, Reddit, Netflix, GitHub and more. Therefore major parts of the Internet were rendered inaccessible. At this point Mirai had enslaved around $600,000$ IoT devices [18], [20].

In November 2016 another major attack on German Telekom[4] routers was seen. The already existing botnet was scanning Telekom routers for a security flaw in their update mechanism. This flaw would allow malicious attackers to gain access to the device – and make them join the Mirai botnet. Despite that not all devices were vulnerable to this security flaw, the immense probing and trying to access the port by the botnet, overloaded thousands of Telekom routers. These routers were then not able to function ordinary and this resulted in an Internet outage for thousands of Telekom customers all over Germany.

[1] a network of Internet-connected devices which have been breached and can be controlled remotely
[2] a French cloud computing company which offers virtual private servers
[3] publishes leaks and classified documents
[4] largest Internet service provider in Germany

At the end of 2017 three suspects pleated guilty to all of the above outlined attacks. Brian Krebs conducted some in-depth investigation which then consequently allowed to discover the attackers in cooperation with international police forces [18].

None of the attacks were political motivated. They either wanted to grow the botnet, or attack hosting services to create outages and downtimes for specific targets. These targets were often given by customers who paid for this service – in the Dyn and OVH case to stop a competing Minecraft[5] server [21].

B. Mira Methodology

The source code of the original Mirai was posted in a forum at the end of September in 2016 [6]. This allowed an in-depth analysis of the methodology of Mirai.

Mirai targeted a wide audience of device types – covering ARM, ARM7, MIPS, PPC, and x86 architectures using a firmware based on Linux. The idea was to create a simple botnet which infects heterogeneous devices, like IP cameras, routers, printers and more.

Usually the usage of network address translation (NAT) in routers protects individual devices device by being accessed from the Internet. However, the feature Universal Plug and Play (UPnP), which is often by default enabled on routers, allows devices to automatically communicate with routers and open certain ports to make the device accessible from the Internet. This is done automatically, as a convenience features for users, to allow the usage of all advertised features. The results are numerous devices which are accessible from the Internet.

Internet-wide scanning of devices and their open ports allowed the initial Mirai devices to search for devices which were accessible on the Internet and exposing certain network services like `telnet` or `ssh`. By then using 64 different default username-password combinations, seen in Figure 4, the devices were compromised. The complete access then allowed to execute the malware and enslave the device.

The already enslaved IoT devices were used for Internet-wide scanning and search for exposed ports and network services. When a device was found which allowed the authentication by using one of the 64 username-password combinations, this device was reported to the report server. The report included the victims IP address and the working credential combination. The report server then injected the malware into the vulnerable device. The malware allows the control of the IoT device – it is now part of the botnet. Furthermore the malware also fixed the used security issues – either by changing the credentials or closing the network service. This is an important feature, as malware based on Mirai were after the open source release competing for IoT devices. This process is displayed in Figure 5.

Figure 6 displays the command and control module of Mirai. This structure is the typical command and control (C&C) structure. The botmaster has access to the C&C server which controls and commands the bots. These bots then for example attack selected victim sites. This architecture enables the botmaster to stay anonymous as all attacks are proxied through the bots [17]–[19], [22].

The methods of Mirai are still widely used and inspired dozens of new malware, due the simplicty and effectivness of Mirai [18].

[5]popular computer game of Microsoft

[6]`https://github.com/jgamblin/Mirai-Source-Code`

Username/Password	Manufacturer
admin/123456	ACTi IP Camera
root/anko	ANKO Products DVR
root/pass	Axis IP Camera, et. al
root/vizxv	Dahua Camera
root/888888	Dahua DVR
root/666666	Dahua DVR
root/7ujMko0vizxv	Dahua IP Camera
root/7ujMko0admin	Dahua IP Camera
666666/666666	Dahua IP Camera
root/dreambox	Dreambox TV receiver
root/zlxx	EV ZLX Two-way Speaker?
root/juantech	Guangzhou Juan Optical
root/xc3511	H.264 - Chinese DVR
root/hi3518	HiSilicon IP Camera
root/klv123	HiSilicon IP Camera
root/klv1234	HiSilicon IP Camera
root/jvbzd	HiSilicon IP Camera
root/admin	IPX-DDK Network Camera
root/system	IQinVision Cameras, et. al
admin/meinsm	Mobotix Network Camera
root/54321	Packet8 VOIP Phone, et. al
root/00000000	Panasonic Printer
root/realtek	RealTek Routers
admin/1111111	Samsung IP Camera
root/xmhdipc	Shenzhen Anran Security Camera
admin/smcadmin	SMC Routers
root/ikwb	Toshiba Network Camera
ubnt/ubnt	Ubiquiti AirOS Router
supervisor/supervisor	VideoIQ
root/<none>	Vivotek IP Camera
admin/1111	Xerox printers, et. al
root/Zte521	ZTE Router

Fig. 4. The 64 username-password Combinations Used by Mirai (taken from [22])

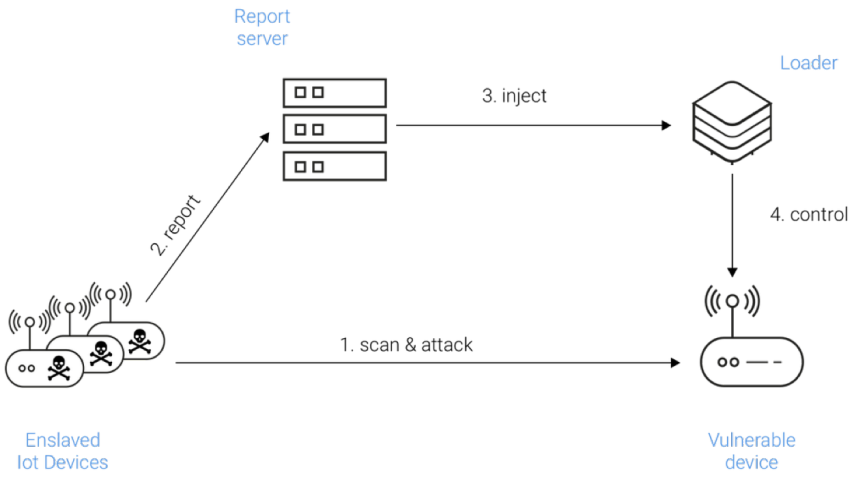

Fig. 5. Scan And Replicate Module of Mirai (taken from [17])

IV. Mitigations

This section will present mitigations for making the IoT more secure and reliable. It is divided into two subsections: Technical Mitigations and Policy Mitigations.

The presented mitigations always involve engineering work. IoT security always comes at a cost – developments costs, hardware costs and more.

A. Technical Mitigations

As presented in the previous sections, and especially in the subsection II-E, the most common and most serve security issues are usually not complex unsolved technical problems – quite the contrary. For all presented security issues, technical mitigations do exist and are the default in traditional IT devices. In the security community this is often called *good security*

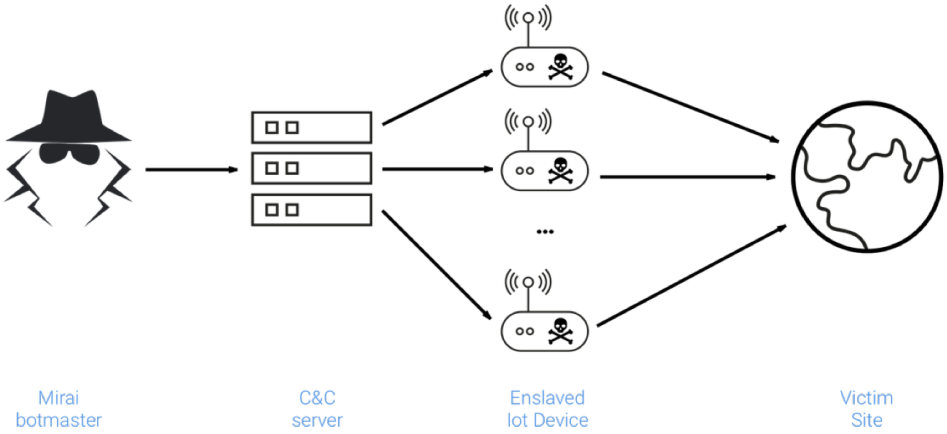

Fig. 6. Control And Attack Module of Mirai (taken from [17])

practice. Good security practices include a number of practices which have been developed over the last decades from the most popular vulnerabilities [2], [6], [10].

In the following subsections I will outline four of the most common.

1) Weak passwords: By using default, or hard coded passwords, malicious attackers can use targeted attacks against known device by trying the default username password combinations. Furthermore when malicious attackers try to gain access to the device by *guessing* the password, they can limit their guesses to known popular passwords. The emergence of botnets, like the Mirai botnet, was only possible due to hard coded default passwords. Using randomly created passwords, or forcing the user to set strong passwords would already have mitigated the emergence of multiple botnets [6], [10], [13].

2) Exposing network services: Network services are essential for some features of IoT devices. Nonetheless these network services need to be secured by authentication mechanism and should be limited to the specific feature – not allow complete access to the device. Often recommended is the usage of default turned off network services and only turn on the necessary services which are needed for specific features.

Furthermore to limit the access to the local network, UPnP should not be used automatically. Often IoT devices use UPnP without the specific confirmation and acknowledgment of the user, which results in an IoT device which is exposing its services to the Internet. Most devices are secured by the NAT of routers, however the usage of UPnP exposes network service to the Internet instead of just the local and network and consequently increases the threat significantly [6], [10], [13].

3) Implementation and usage of standards: In the early phases of the development of IoT devices the industry was still missing standards and frameworks on all presented layers, like operating systems, communication protocols, cryptography libraries etc. As a result engineers often developed their own implementations, like authentication algorithms, or cryptography for embedded systems. This step is in general not recommended, as the implementation of low-level features and security features is complex. Usually it is recommended to use well known standards from e.g. industry cooperations or universities, with multiple developers and which have been used, and therefore proven, for years.

However, in the recent years, IoT standards have been developed for all existing layers – from wireless communication protocols, operating systems for embedded systems, to well

maintained cryptography libraries specialised for limited computing power.

In general, it is always recommended for developers to use existing standards before developing their own. Popular libraries and standards of industry collaborations or open source projects are usually the better choice, as the development is complex, and existing libraries usually have proven them self over the years [6], [10], [13].

4) Automatic updates: Nonetheless, the introduction of good security practices within the IoT will not safeguard the IoT from all risks – it is just the first essential step to make attacks harder. Security research is always an ongoing endeavor and new vulnerabilities are detected daily. Consequently the implementation of automatic security update mechanisms is the next crucial step.

Given the public knowledge of Common Vulnerabilities and Exposuress (CVEs), malicious attacks in the future will use public CVEs. Unpatched IoT devices will always be vulnerable to those security issues and the only way to mitigate is by patching the known issues [18].

Automatic security updates are well known and the default configuration for IT devices – especially in the enterprise configurations. The same development has to happen for IoT devices – preferably without user interaction, so the device automatically applies the most recent security patch [6], [10], [13].

B. Policy Mitigations

The introduction of policies by regulators or government authorities is essential for reducing the risks of IoT devices for the Internet, but also the privacy of users. At present there is little incentive for manufactures to use good security practices, as they increase the development time, and time to market is critical for trends like the IoT [9], [12].

Furthermore, the market has an increased demand for more secure devices and consumers are caring, however most consumers are not able to understand the security of IoT devices and lack the knowledge and skills. Consumers have no accessible way to rank IoT devices by their security features. Therefore the development and enforcement of strong and robust security standards (for the IoT) is essential.

1) Policy proposals: The authors of [12] propose a Consumer Security Index (CSI) which they co-developed with consumers and security experts. The goal is to help consumers decision making regarding buying an IoT device. At the moment it is hard for consumers to make informed decisions about the security of an IoT device. Usually consumers lack the knowledge to make informed decisions. The general idea for the CSI is to create a metric to rank the security of an IoT device and therefore incentivise the consumers to focus on greater security. Furthermore manufactures can use the CSI as a marketing tool and to differentiate themselves from competitors.

Indexes similar to CSI do already exist – an example is the energy efficiency label of the European Union, seen in Figure 7. White goods, light bulbs, cars and more are required to display their energy label which indicates the energy efficiency of the device from A to G. Furthermore the label also presents further information which allows the consumer to differentiate between the energy efficiency of competing devices. The introduction of this label lead to the choice of more energy efficient devices [24].

The proposal of the CSI has a similar goal – lead consumers to buy more secure devices, but also set incentives for the manufactures to develop more secure devices and advertise it as a key feature [9], [12], [25].

2) Policy risks: The usual problems with regulations arise – regulations are usually only valid country wide. If fortunate, regulations can be introduced by unions like the European

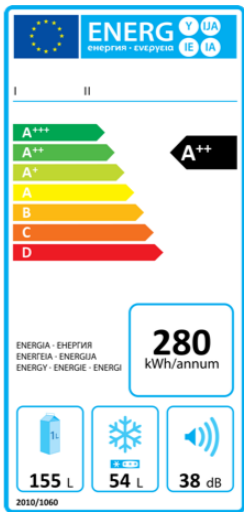

Fig. 7. EU Energy Label (taken from [23])

Union or trade unions and be included in trade policies. This would increase the leverage significantly and the interest of manufactures to enter the regulated markets.

Furthermore, introducing policies might allow users to easier judge the security of an IoT device – for example by introducing the CSI. However, consumers still need to care about privacy and the risks introduced by the IoT. Therefore more consumer education about the risks of privacy intrusion and other risks from IoT devices is necessary.

Introducing a single score for measuring the security of a device is not possible, it is always a heuristic. No system can have the property secure – it is not a lifelong property. Secure is just a current status up to the best current knowledge of experts. This trait will make the introduction of automatic security updates even more vital.

At this point in time, the interests in consumer protection policies regarding IoT has increased, however, current regulations are mostly the reason of the interest of national defense agencies which want to enforce strong regulations on IoT device for cybersecurity defense. The introduction of the IoT has also increased the thread to nations, as other (state sponsored) malicious actors can also use vulnerable IoT devices. California just introduced a law [26] and the National Institute of Standards and Technology released some considerations on IoT devices for government institutions [11]. This trend by government and defense institution will continue in the future [27]. California's law for example states: *'the preprgogrammed password is unique to each device manufactured'*. Summarized the law introduced some features of what we covered as good security practices.

V. Conclusion

This seminar report has summarised the current landscape of IoT security, discussed the challenges which were introduced by IoT devices, and lastly discussed technical and policy mitigations for a more secure IoT.

The IoT changed the security landscape dramatically. The numbers of devices is still growing exponentially, and the diversity of devices is continuing to increase. IoT devices have infiltrated the everyday life with enormous consequences. A new type of Internet was introduced – more heterogeneity, a more complex network, and overall more devices.

As discussed, the given hardware challenges create a barrier for implementing and the use of good security practices – like the limited computing power or the need of energy efficient devices. Heterogeneity and complexity make IoT security more difficult than previous trends [10]. However, in recent years multiple frameworks and platforms were introduced which now enable a solid framework for developing IoT devices. Furthermore market incentives were also pulling in favor of insecure devices. Implementing security always comes at a cost which then will increase the time to market. In addition consumers usually can not judge which IoT device is more secure, as the knowledge is not available and for non-experts hard to understand. The mentioned reasons resulted in networks with insecure IoT devices. This enabled new powerful attacks on the Internet and computer networks, as described in the example of the Mirai botnet.

Furthermore, given by the definition of sensing and interacting with the physical world, IoT devices allow for a never seen before privacy intrusion. Compromised IoT devices do not only allow the access to the device itself, they enable access to the data, but also to the sensors which usually monitor physical spaces – starting from eavesdropping to controlling the thermostat in the living room.

In the last section possible mitigations were presented. The current IoT threats and malware are not highly sophisticated technical attacks – already the introduction of good security practices would omit most of the presented security risks in IoT device.

However, once good security practices have been introduced and deployed, this problem will get more complex similar to the trend in traditional IT equipment. Complex zero-days vulnerabilities will be used more common. Therefore the implementation of automatic security updates is the next crucial step – as it is already done on common operating systems for IT equipment.

On the whole, it is important to point out that the lack of security in IoT devices at the current point in time is not due to missing technical solutions, or complex technical problems. As discussed, the technical mitigations have been known for years and are in general collected under the term *good security practices*.

Consequently, this report also presented possible policy mitigations. The introduction of policies or government regulations is a key factor to set incentives for manufacture to focus on good security standards to protect consumers. They should enable consumers to either have a simple metric to judge the security of the device, or only allow approved and tested IoT devices on the market – similar to other markets which are regulated for the security of all.

Appendix A
OWASP Top 10

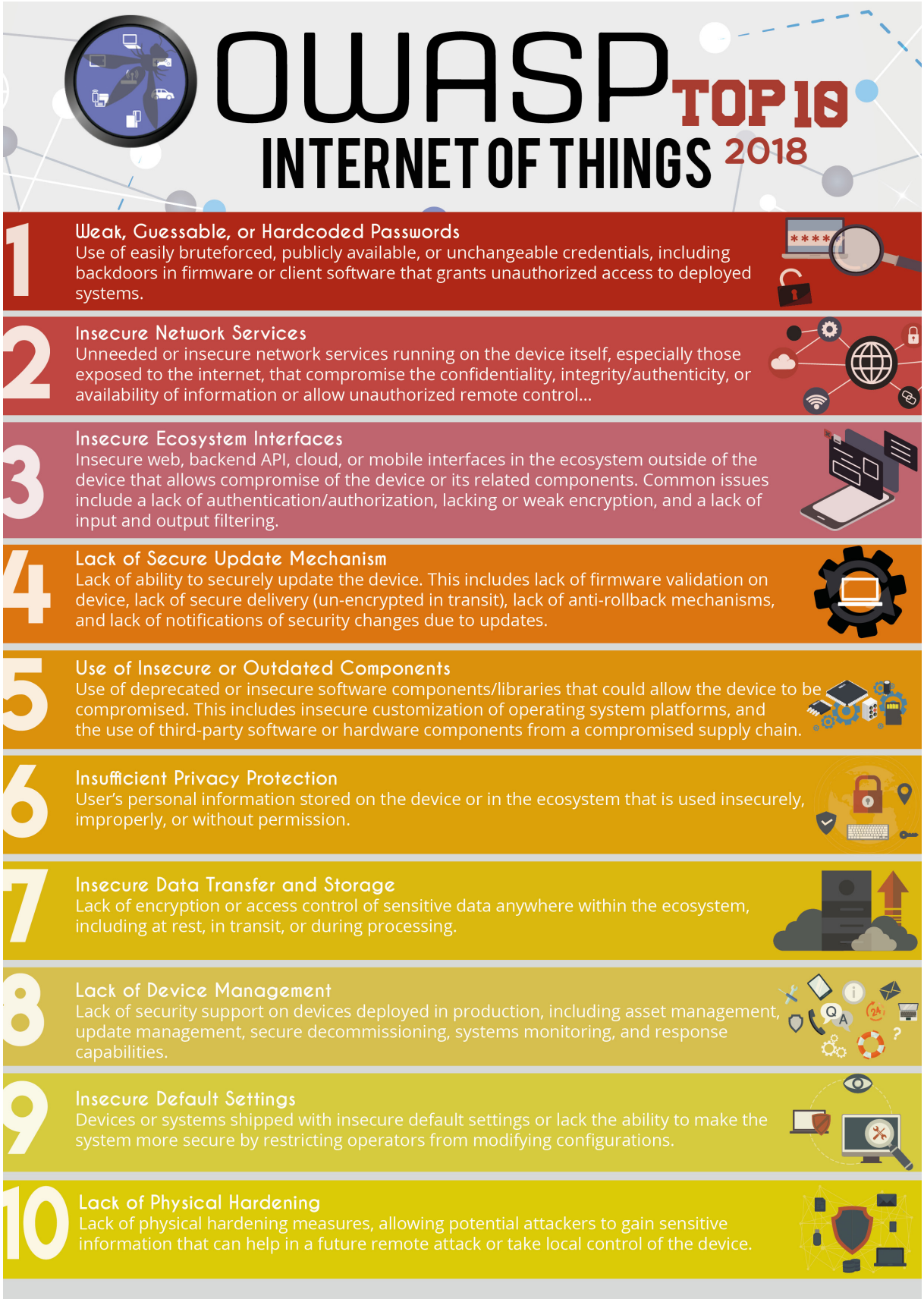

Fig. 8. OWASP Top 10 (taken from [13])

Appendix B
Abbreviations

IoT	Internet of Things
OS	operating system
DNS	domain name server
malware	malicious software
DDoS	distributed denial-of-service
C&C	command and control
NAT	network address translation
OWASP	Open Web Application Security Project
UPnP	Universal Plug and Play
CSI	Consumer Security Index
CVE	Common Vulnerabilities and Exposures

List of Figures

REFERENCES

[1] "Internet of Things forecast – Ericsson Mobility Report," Oct 2019, [Online; accessed 15. Oct. 2019]. [Online]. Available: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

[2] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti, "A large-scale analysis of the security of embedded firmwares," in *23rd USENIX Security Symposium USENIX Security 14*, 2014, pp. 95–110.

[3] S. Oh and Y. Kim, "Security requirements analysis for the iot," in *2017 International Conference on Platform Technology and Service (PlatCon)*, Feb 2017, pp. 1–6.

[4] "IoT: Security Introduction," Dec 2019, [Online; accessed 8. Dec. 2019]. [Online]. Available: https://jan.newmarch.name/IoT/Security/Security

[5] A. Calihman, "IoT Architectures - Common Approaches and Ways to Design IoT at Scale," *NetBurner*, Jan 2019. [Online]. Available: https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization

[6] K. Zhao and L. Ge, "A survey on the internet of things security," in *2013 Ninth International Conference on Computational Intelligence and Security*, Dec 2013, pp. 663–667.

[7] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "Dolphinattack: Inaudible voice commands," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, pp. 103–117.

[8] A. Costin and J. Zaddach, "Iot malware: Comprehensive survey, analysis framework and case studies," *BlackHat USA*, 2018.

[9] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, Oct 2017.

[10] Z. Zhang, M. C. Y. Cho, C. Wang, C. Hsu, C. Chen, and S. Shieh, "Iot security: Ongoing challenges and research opportunities," in *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, Nov 2014, pp. 230–234.

[11] K. R. Boeckl, M. J. Fagan, W. J. Fisher, N. B. Lefkovitz, K. N. Megas, E. M. Nadeau, B. M. Piccarreta, D. G. O'Rourke, and K. A. Scarfone, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks," Jan 2020, [Online; accessed 2. Jan. 2020]. [Online]. Available: https://www.nist.gov/publications/considerations-managing-internet-things-iot-cybersecurity-and-privacy-risks

[12] J. Blythe and S. Johnson, "The consumer security index for iot: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in iot devices," 2018.

[13] "OWASP Internet of Things Project - OWASP," Nov 2019, [Online; accessed 8. Dec. 2019]. [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[14] "New Mirai Worm Knocks 900K Germans Offline — Krebs on Security," Dec 2019, [Online; accessed 8. Dec. 2019]. [Online]. Available: https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline

[15] "IoT threats: Explosion of 'smart' devices filling up homes leads to increasing risks - F-Secure Blog," Apr 2019, [Online; accessed 8. Dec. 2019]. [Online]. Available: https://blog.f-secure.com/iot-threats

[16] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[17] E. Bursztein, "Inside Mirai the infamous IoT Botnet: A Retrospective Analysis," *Elie Bursztein's site*, Dec 2017. [Online]. Available: https://elie.net/blog/security/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis

[18] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the mirai botnet," in *26th USENIX Security Symposium USENIX Security 17)*, 2017, pp. 1093–1110.

[19] "Who is Anna-Senpai, the Mirai Worm Author? — Krebs on Security," Oct 2019, [Online; accessed 15. Oct. 2019]. [Online]. Available: https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author

[20] "DDoS on Dyn Impacts Twitter, Spotify, Reddit — Krebs on Security," Dec 2019, [Online; accessed 8. Dec. 2019]. [Online]. Available: https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit

[21] L. Mathews, "Angry Gamer Blamed For Most Devastating DDoS Of 2016," *Forbes*, Nov 2016. [Online]. Available: https://www.forbes.com/sites/leemathews/2016/11/17/angry-gamer-blamed-for-most-devastating-ddos-of-2016/#1489cf0c2dac

[22] "Who Makes the IoT Things Under Attack? — Krebs on Security," Dec 2019, [Online; accessed 8. Dec. 2019]. [Online]. Available: https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack

[23] "European Union energy label - Wikipedia," Nov 2019, [Online; accessed 8. Dec. 2019]. [Online]. Available: https://en.wikipedia.org/wiki/European_Union_energy_label?oldformat=true

[24] "Study on the impact of energy label – and potential changes to it consumer understanding purchase decisions - Energy European Commission," Jan 2015, [Online; accessed 8. Jan. 2020]. [Online]. Available: https://ec.europa.eu/energy/en/studies/study-impact-energy-label-%E2%80%93-and-potential-changes-it-%E2%80%93-consumer-understanding-and-purchase

[25] J. A. Jerkins, "Motivating a market or regulatory solution to iot insecurity with the mirai botnet code," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan 2017, pp. 1–5.

[26] A. Robertson, "California just became the first state with an Internet of Things cybersecurity law," *Verge*, Sep 2018. [Online]. Available: https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law

[27] P. Radanliev, D. De Roure, S. Cannady, R. M. Montalvo, R. Nicolescu, and M. Huth, "Economic impact of IoT cyber risk - analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance," *IET Digital Library*, p. 3(9pp.), Jan 2018.