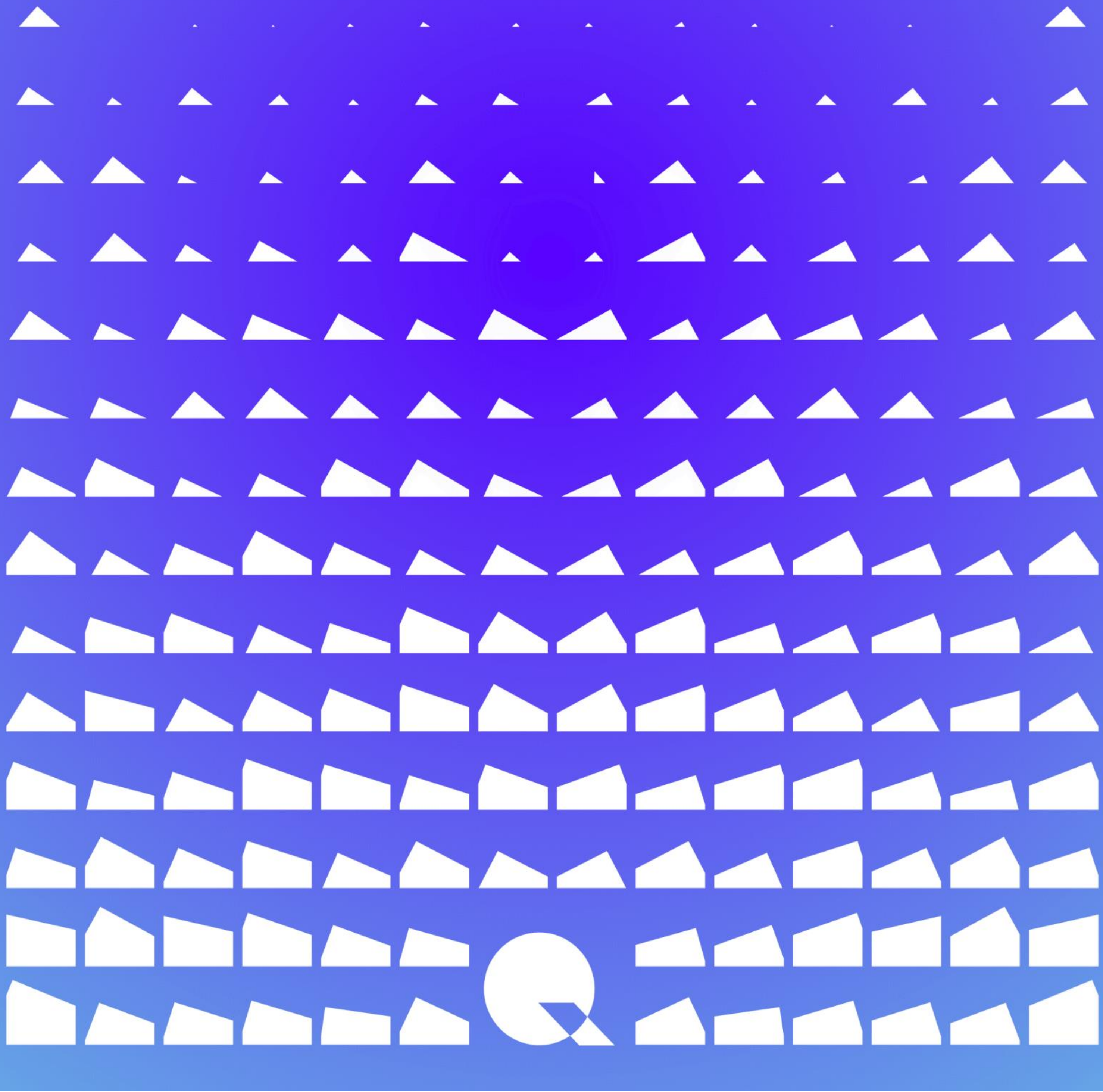
Qbit
CYBER SECURITY

Essential requirements for securing IoT consumer devices

Member of the eurofins Group



Essential requirements for securing IoT consumer devices

Details	
Authors	Pieter Meulenhoff Sjoerd Langkemper Willem Westerhof
Date	6 August, 2020
Report	AGENT-2001-11.010

Table 1: Details of the report.

Samenvatting

Consumentenelektronica bestaat in toenemende mate uit computers die met het internet verbonden zijn, in de vorm van IoT apparaten. Deze apparaten zijn vaak onvoldoende beveiligd tegen cyberaanvallen. Dit onderzoeksrapport stelt enkele veiligheidsvereisten op voor huishoudelijke IoT apparaten. Deze veiligheidsvereisten zijn geschikt om aan fabrikanten op te leggen als regelgeving, en naleving hiervan zal de veiligheid van huishoudelijke IoT apparaten aanzienlijk verbeteren.

Dit onderzoeksrapport, in opdracht van Agentschap Telecom, beschrijft aanvalsscenario's en belangrijke veiligheidsproblemen in de context van consumenten-IoT, naar aanleiding van literatuuronderzoek. Deze scenario's en problemen helpen bij het evalueren van meer dan 400 maatregelen, waarna de beste maatregelen samengevat worden als minimum vereisten. De vereisten zijn makkelijk te implementeren, makkelijk te testen, duidelijk, en vergroten de cyberveiligheid van de producten aanzienlijk. We raden dan ook aan om de vereisten via regelgeving op te leggen voor alle consumenten IoT apparaten.

De volgende maatregelen worden als basis voorgesteld:

- Alle wachtwoorden moeten voldoen aan de standaard NIST SP800-63b Digital Identity Guidelines.
- Na initiële configuratie moeten wachtwoorden uniek zijn voor elk apparaat, of opgegeven zijn door de gebruiker.
- Netwerktoegang tot een apparaat in functionele staat moet alleen mogelijk zijn na authenticatie.
- Het apparaat mag alleen poorten en koppelingen aanbieden die noodzakelijk zijn voor normale en bedoelde functionaliteit.
- Al het netwerkverkeer moet versleuteld en geauthentiseerd worden door middel van gangbare encryptie protocollen, zoals TLS.
- Fabrikanten moeten een update van de programmatuur in apparaten kunnen initiëren. Doormiddel van automatische updates, ofwel door het actief informeren van de eindgebruiker.
- Het apparaat moet de integriteit en authenticiteit van programmatuur controleren alvorens deze te installeren.
- De fabrikant moet duidelijke informatie verschaffen over de verantwoordelijkheden van de eindgebruiker om het apparaat veilig te gebruiken.

Abstract

Embedded connected computers are installed in homes in increasing numbers in the form of consumer IoT devices. These devices are often insufficiently protected against cyberattacks. In this research report, we propose several security requirements for consumer IoT devices. These requirements are suitable for enforcement through legislation and will significantly improve consumer IoT cybersecurity when implemented.

This research report, commissioned by the Dutch Radiocommunications Agency, describes a threat model and significant security problems, derived from literature research. These assisted in evaluating more than 400 security measures, after which the top measures were summarised into eight essential security requirements. These requirements are easy to implement, easy to test, unambiguous, and greatly improve the cybersecurity of the products. We recommend standardisation agencies to make these requirements mandatory for all consumer IoT devices.

The following basic requirements were described:

- All passwords must conform to the industry standard NIST SP800-63b Digital Identity Guidelines.
- After initial setup, passwords must be unique for each device, or defined by the user.
- Access to device functionality via a network interface in the initialised state must only be possible after authentication on that interface.
- All exposed ports and interfaces must be necessary for the normal and intended use of the device.
- All network traffic must be encrypted and authenticated using best practice encryption protocols, such as TLS.
- Vendors must be able to initiate firmware updates in IoT devices, either by automatic updates or by actively informing the user about availability of updates.
- The device must verify the authenticity and integrity of firmware updates before installing them.
- The vendor must provide clear and understandable information about the end user’s responsibilities to set up and maintain the device’s privacy and security.

Table of contents

List of tables

List of figures

1 Introduction

The Internet-of-Things (IoT) is one of many exciting innovations that connects humans with technology, both at home and in business. It offers the potential for seamless interaction between humans and almost any device. Combined with machine learning and artificial intelligence, IoT creates vast opportunity for innovators, law-abiding citizens, mischief makers and criminals alike. Given the number of cyber security breaches reported each day, the well-published lack of investment in security and a shortage of security staff, one may ask whether the benefits of IoT can be achieved safely, or whether more consideration is needed to understand IoT risk.

In the 'Staat van de Ether', Radiocommunications Agency Netherlands has, in recent years, advocated to improve the security of IoT devices [1] [2]. An investigation in 2019 commissioned by the Radiocommunications Agency evaluated the cybersecurity of 22 consumer IoT devices. The findings of this assessment confirm that, in general, security of IoT devices is not sufficient [3].

For consumers, it is difficult to evaluate the security of a product when buying the device. If the security is poor and the device is abused, the owner of the device may not be aware, even when the device is used to attack other hosts on the internet. Since the market insufficiently favours secure products, there is a possibility for legislation to improve cybersecurity of consumer devices.

Several sources emphasize the role of the government and the importance of regulations on the IoT market [4], [5], [6]. In 2017, Senator Warner introduced a bill in the United States senate, stating four security requirements for IoT devices [7]. The United Kingdom has plans to introduce three mandatory security requirements for IoT [8].

The European Commission aims to improve the digital security of devices, for example through legal requirements such as the Radio Equipment Directive (RED). Where RED 2014/53/EU [9] establishes a regulatory framework for placing radio equipment on the market, the specifications of technical requirements are put up by the European standardisation organisations ETSI, CEN and CENELEC.

This standardisation effort can benefit from a well-founded set of essential requirements for IoT devices. This report provides an overview of vulnerabilities found in various studies and the security requirements that are assumed herein. This to finally arrive at a well-weighted and substantiated set of requirements for a standard framework for cyber-safe IoT equipment.

1.1 Objective

The objective of this report is to present a well-founded set of essential security requirements to improve the security of consumer IoT devices. The security requirements are meant to be implemented by vendors and verified by other parties, possibly without cooperation from the vendor. These security requirements are based on literature research on IoT vulnerabilities, followed by a requirements analysis of available security measures and recommendations. The main research question is:

Which specific security requirements are most effective in improving the security of consumer devices?

The objective is thus to provide a relatively small set of requirements, that will effectively improve the cybersecurity of consumer devices. To determine which requirements are most effective, we investigate which threats and vulnerabilities are relevant to our scope, by answering the following research questions:

- Which threat model is applicable to consumer IoT devices?
- What are the most severe vulnerabilities in consumer IoT devices?

1.2 Scope

The security requirements proposed in this report are a set of essential requirements. The goal is to eliminate those security vulnerabilities that impose the highest security risks. This set of requirements does not aim to eliminate all the security issues present in consumer IoT devices.

This report focuses on consumer IoT devices as used in the home environment. Most of these devices are connected to a network, such as the Wi-Fi network of the end-user. Examples include cameras, baby monitors, smart locks, smart thermostats, toys and routers. IoT used in other environments, such as industrial IoT, is not considered.

Consumer IoT devices can be deployed in large numbers, where a single vulnerability can affect hundreds of thousands of devices. Consumer devices are typically present in the home, and store personal information, making privacy an important issue. Using an IoT device for important day-to-day activities such as locking the house or controlling heating makes disruptions in service very inconvenient, and perhaps dangerous. Many IoT devices are mains powered and connected to the internet, making them an attractive target for abuse.

The purpose of this report is to suggest security requirements for vendors to implement in their devices. This means that only requirements over which the vendor has control are suitable. For example, several sources [10] [11] advocate for intrusion detection in networks where IoT devices are deployed. However, vendors of consumer devices have little control over the network in which devices are deployed, and whether that network is equipped with intrusion detection.

1.3 Reading guide

The remainder of this report describes the methodology in chapter 2, Method. The relevant threat model and most severe vulnerabilities are discussed in chapter 3, IoT vulnerabilities. Chapter 4, Requirements analysis, evaluates security measures and provides the basic set of security requirements. Finally, chapter 5 concludes and provides recommendations.

2 Method

We evaluated security measures and summarised the best security measures into basic security requirements. To support the evaluation, we determined a threat model and a list of most important security problems.

2.1 Literature research

This study is primarily based on literature research. We used Google Search, Google Scholar, Qwant, IEEE Xplore, and the ACM Digital Library to identify relevant sources. The primary focus of the literature search is to find publications that provide a well-founded insight to the security problems of consumer IoT. We attempted to identify sources that provide:

- an overview of the state of IoT security;
- information on actual attacks;
- information on actual vulnerabilities in devices;
- categories of IoT security problems;
- security measures or recommendations to improve IoT security;

Of the 71 found sources, 58 are cited in this report. The other sources were not applicable to our scope or threat model. For example, several sources describe methods to detect attacks on a network by analysing traffic. However, this is not under control of a device vendor, and therefore not applicable in our research.

The literature used for this research consists of a wide range of sources such as academic, commercial, consumer organisations and vulnerability disclosures. Where possible, we preferred academic publications. However, certainly in the case of actual attacks and vulnerabilities, academic publications were not always available. An exception to this is the Mirai botnet, which was significantly disruptive, and several academic papers were published about it.

Since IoT and cybersecurity are both innovating fields, we preferred recent sources, published in the last four years. Of our 71 sources, 58 are published in 2016 or later.

The result of the literature search was condensed into two sets: a description of the threat model and a list of security problems in consumer IoT. Where the threat model focusses on describing the most important security threats and attack patterns, it lacks a mapping to root cause problems. The latter is the topic in the overview of vulnerabilities, which describes the most important security problems in consumer IoT. The most important vulnerabilities were selected based on their security risk as found in literature.

2.2 Determining threat models

The threat model identifies the most likely attack vectors. We wanted to provide security requirements to improve the security of IoT products. For this, it is important to know against which kinds of attacks IoT equipment should be protected. For example, restricting network access may protect against attackers from the internet, but not from an adolescent who wants to use his SmartTV past his bedtime.

To determine threat models, we looked at actual attacks and vulnerabilities as described in literature. Several sources also describe their threat model, and one sufficiently matched the actual attacks and vulnerabilities that we adopted it as our threat model [12]. The threat model can be found in section 3.2.

2.3 Determining IoT security problems

The proposed essential security recommendations aim to resolve the most important IoT security problems. To evaluate this, we needed a list of those problems, preferably in order of relevance.

Several of the sources from the literature research provided categorisations of IoT vulnerabilities [12] [13] [14] [15] [16]. Even though we would have preferred to use a canonical categorisation from one of these sources, the categories proposed in these sources were not sufficiently useful for our purpose. Most sources attempt to provide an exhaustive list of problems, instead of listing the problems with the most impact. This leads to problems that are not applicable to our threat model. Furthermore, several proposed categories are scoped too narrowly or too broadly, which would give problems when checking whether a measure adequately solves the problem.

Our approach is to combine categories from these publications into a new problem taxonomy. We started with the categories described in [14]. We removed problem categories that were not relevant to our threat model. We combined and split categories to make them similar in scope, and sufficiently specific to evaluate security measures against. After checking this list against several other sources [17] [18], we added several problem categories.

We ordered the list of problems based on the prevalence and impact of each problem, as derived from literature. We placed problems that were exploited in an actual attack at the top. This ordering is not absolute, since sources disagree on what the largest problems are, and attacks can be mapped to problems in multiple ways.

2.4 Determining sources for candidate security measures

To get a set of basic security requirements, we evaluated many candidate measures and selected those that did best in the evaluation. The evaluated measures originate from well-known lists of security measures or recommendations by respected sources, which are used in the IoT market.

Several papers that discuss IoT security problems also provided recommendations [12] [19] [20]. We did not include these as candidate measures. First, we feel these are not as reputable and well known as e.g. ETSI and ENISA. Second, it is likely that these recommendations have significant overlap with our candidate measures.

In addition to the sources described in section 4.3, we also considered using NIST's Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things [21]. However, this report does not provide specific recommendations to improve security of IoT devices and was thus not useful as a source of security measures.

2.5 Evaluating candidate security measures

We evaluated the security measures, and ordered them on score, so that the best measures were at the top. To evaluate each candidate measure, we scored each measure on several attributes. These attributes were designed to match the intended use of the basic requirements in practice. For example, it must be possible for vendors to widely implement the requirements, and for standardisation agencies to verify whether the requirements have been implemented.

A detailed overview of the evaluation criteria is provided in section 4.2. For each measure, these criteria were evaluated, and a score was calculated. A measure with a higher score is better.

The scoring method we used gave a particular ordering of security measures. To ensure that this ordering correctly reflected our evaluation criteria, we experimented with an alternative scoring method. This way, we could determine how the results varied and the dependence on the used scoring method.

While the goal is to provide a set of most effective security requirements, all background material is provided in such a way that the study allows the possibility to select requirements on other criteria, such as efficiency (required implementation effort versus effectivity).

2.6 Selecting top security requirements

Next, we determined how many of the top security measures to select as our basic requirements. Using somewhere between three and thirty measures seemed sensible. When more than 100 measures are given, it is no longer a basic set to solve the most important problems. To determine how many candidate measures to use, we looked for a sudden drop-off in score. We plotted the scores on a chart, shown in section 4.6, and selected the measures before the first drop-off.

2.7 Summarizing basic requirements

The previous step resulted in a small set of security requirements. However, since these are obtained by taking a small part of several sources, the requirements overlap or are inconsistent with each other. We combined and summarised the requirements, to end up with a consistent set of requirements.

3 IoT vulnerabilities

3.1 Introduction

Requirements for IoT security must be focussed on preventing or resolving security vulnerabilities. To create an effective set of security requirements, knowledge is required of the most important security threats and their root cause. Providing insight to the security threats and problems in consumer IoT is the goal of this chapter. Section 3.2 answers the research question: which threat model is applicable to consumer IoT devices? Section 3.3 answers the question: what are the most severe vulnerabilities in consumer IoT devices?

3.2 Threat model

Review of literature of attacks and vulnerabilities in IoT showed that IoT devices that are connected to the internet can be successfully attacked remotely [16] [19] [22]. A malicious actor can attack devices over the internet. Attacks over the internet seem most prevalent and impactful. It is easy to target many devices in this way.

Some sources assume another threat model, in which the attacker needs to be physically close to the victim's device [23], or where the attacker can intercept the traffic of the devices [24]. Even though these sources describe actual vulnerabilities, actual attacks described in literature exclusively work by attacking devices over the internet.

Besides the attack method, attacks differ in the goal of the attacker. Of course, an attacker can obtain access to an IoT device and obtain sensitive information from it. However, in several attacks, the IoT device is not the intended target, but used as a tool in another attack. This supports two attack scenarios that appear to be the dominant attack patterns [12].

From a security perspective, an important pattern is the ubiquity of inexpensive IoT devices, which means that a large number of similar devices are connected to the Internet. The recent history has demonstrated that large-scale attacks on these can spread like a virus and have a significant impact [25]. These types of attack, targeted at devices with an internet connection, are interesting to attackers as they seek to infect other targets and thereby amplify their impact. The next section expands on that attack scenario.

The other dominant attack scenario is where the goal is to gain control over a device or extract information from it. In these cases, attacks are directly targeted at the devices themselves and directly affect consumer-privacy, personal finance and physical security.

3.2.1 Home IoT as an attack amplifier

When many devices are compromised, these can be abused to amplify the intent of the attacker. The impact originates from compromising many devices that simultaneously execute a cooperated attack. The compromised devices form a botnet, which can be centrally controlled by an attacker. This is typically abused to perform a distributed denial of service (DDoS) attack. While the traffic that a single device can generate is negligible, thousands of devices together can send a crippling amount of traffic to a victim, thereby disrupting their accessibility. Other possible attacks include sending spam messages or performing brute-force attacks on authentication mechanisms.

Even though infecting many devices is possible with a central attack, a distributed attack can make malware spread like a virus. After a device is infected, it searches on the internet and the local network for other vulnerable devices and infects them as well. IoT devices are typically sufficiently versatile that they can run arbitrary software, which means that the attacker can install his own programs and make the device perform malicious functionality not intended by the vendors.

This attack scenario depends on thousands of compromised devices. Some devices are so ubiquitous that targeting a single device type or exploiting a single vulnerability leads to sufficiently many compromised devices to form an effective botnet. For example, in an attack in 2016, 900,000 routers were disabled by a cyberattack [26].

In most cases, the devices keep functioning normally and the user does not notice that their device is compromised [27] [28]. In home and small office environments, outgoing network traffic is often insufficiently monitored to notice that the device is being abused in an amplification attack.

One example of an attack on many devices that were subsequently commandeered in amplification attack is the Mirai botnet. It infected approximately 600,000 internet-connected devices by authenticating with default credentials. These hacked devices subsequently performed some of the largest DDoS attacks ever [19] [29].

Besides amplifying internet traffic, devices can also amplify power usage. By switching many devices on and off simultaneously, it is possible to disrupt the power grid and cause a power outage [30] [31].

3.2.2 Home IoT as an attack target

The attacks in this scenario are directly targeted at the IoT devices themselves. The impact of attacks in this scenario is usually restricted to the end user of the device and typically results in disclosing sensitive information or obtaining control over an IoT device.

Several reports are available on unauthorised access to home camera systems [32] [33]. This typically results in cases where anyone can view people and their activities in their own house, directly violating their personal privacy. Information about activity in the home and storage locations of valuable items could assist in home invasion and robbery.

In a thorough analysis of vulnerabilities and attack scenarios against 499 smart home control applications and 132 device handlers, more than 55% of the examined applications were over-privileged and lacked basic protection mechanisms [34]. It was possible to obtain sensitive information such as door lock codes, gain control over home surveillance system, disable the vacation mode and issue fake fire alarms.

Other security tests conducted on smart TVs uncovered vulnerabilities where plain-text HTTP traffic was transmitted over the Internet [35] [36]. By staging a Man-in-the-Middle (MitM) attack, the unencrypted traffic could be manipulated or redirected to malicious websites, resulting in gaining control over the Smart TV. In other attacks, the DVB-T signal was manipulated resulted in obtaining control over a television [37].

3.3 The most important IoT security problems

This section categorises the most pressing problems in consumer IoT. These problems are the most important that relate to the attack scenarios defined in the previous section. Insight to these problems will facilitate evaluating requirements in the next section, by reflecting how well implementing the requirement would solve problems from the categories listed here.

As described in section 2.3, these categories were adapted from one survey [14], with some modifications to better fit the established threat model and make the scope of the problems consistent.

We omitted the problem of insufficient energy harvesting. In actual attacks, most of the devices are connected to mains power. In battery-powered devices such as smart watches, vulnerabilities were not related to battery power [38].

We changed several problem categories in scope. The problem of unnecessary open ports is generalised to overly large attack surface. The categories of improper update capabilities and improper patch management capabilities were joined into outdated software.

Finally, several problem categories were added, after consulting other sources of common problems [17] [12] [39]:

- Lack of trusted execution environment;
- Vendor security posture;
- Insufficient privacy protection;
- User interaction.

The following sections describe the eleven most common problems. These were generally ordered on severity. The first three problems are relevant to large-scale attacks such as Mirai and related botnets [25] [19]. For the first six a relationship is known with an actual attack or a proof-of-concept of a vulnerability [12].

3.3.1 Incorrect access control

Services an IoT device offers should only be accessible by the owners and the people in their immediate environment whom they trust. However, this is often insufficiently enforced by devices [40].

IoT devices may trust the local network to such level that no further authentication or authorisation is required. Any other device that is connected to the same network is trusted [16] [39].

A common problem is that all devices of the same model have the same default password (e.g. “admin” or “password123”). The firmware and default settings are usually identical for all devices of the same model. Because the credentials for the device are public knowledge, these can be used to gain access to all devices in that series [19].

IoT devices often have a single account or privilege level, both exposed to the user and internally. This means that when this privilege is obtained, there is no further access control. This single level of protection fails to protect against some vulnerabilities [41] [42].

3.3.2 Overly large attack surface

Each connection that can be made to a system provides a new set of opportunities for an attacker to discover and exploit vulnerabilities. The more services a device offers over the internet, the more services can be attacked. Reducing the attack surface is one of the first steps in the process of securing a system.

A device may have open ports with services running that are not strictly required for operation [13] [43] [44]. An attack against such an unnecessary service could easily be prevented by not exposing the service. Services such as Telnet, SSH or a debug interface may play an important role during development but are rarely necessary in production.

3.3.3 Outdated software

As vulnerabilities in software are discovered and resolved, it is important to distribute the updated version to protect against the vulnerability. This means that IoT devices must ship with up-to-date software without any known vulnerabilities, and that they must have update functionality to patch any vulnerabilities that become known after the deployment of the device.

For example, the IoT malware Linux.Darlloz was first discovered late 2013, and worked by exploiting a bug reported and fixed early 2012 [45] [46].

3.3.4 Lack of encryption

When a device communicates in plain text, all information being exchanged with a client device or backend service can be obtained by a Man-in-the-Middle (MitM). Anyone who is capable of obtaining a position on the network path between a device and its endpoint can inspect the network traffic and potentially obtain sensitive data such as login credentials. A typical problem in this category is using a plain-text version of a protocol (e.g. HTTP) where an encrypted version is available (HTTPS) [44].

Even when data is encrypted, weaknesses may be present if the encryption is not complete or configured incorrectly. For example, a device may fail to verify the authenticity of the other party. Even though the connection is encrypted, it can be intercepted by a Man-in-the-Middle attacker.

Sensitive data that is stored on a device (at rest) should also be protected by encryption. Typical weaknesses are lack of encryption by storing API tokens or credentials in plain text on a device. Other problems are the usage of weak cryptographic algorithms or using cryptographic algorithms in unintended ways.

3.3.5 Application vulnerabilities

That software contains vulnerabilities in the first place is an important problem in securing IoT devices [17]. Software bugs may make it possible to trigger functionality in the device that was not intended by the developers. In some cases, this can result in the attacker running their own code on the device [47], making it possible to extract sensitive information or attack other parties.

Like all software bugs, security vulnerabilities are impossible to avoid completely when developing software. However, there are methods to avoid well-known vulnerabilities or reduce the possibility of vulnerabilities. This category includes best practices to avoid application vulnerabilities, such as consistently performing input validation.

3.3.6 Lack of trusted execution environment

Most IoT devices are general-purpose computers that can run arbitrary software. This makes it possible for attackers to install their own software that has functionality that is not part of the normal functioning of the device. For example, an attacker may install software that performs a DDoS attack.

By limiting the functionality of the device and the software it can run, the possibilities to abuse the device are limited. For example, the device can be restricted to connect only to the vendor's cloud service. This restriction would make it ineffective in a DDoS attack since it can no longer connect to arbitrary target hosts.

To limit the software a device can run, code is typically signed with a cryptographic hash. Since only the vendor has the key to sign the software, the device will only run software distributed by the vendor. This way, an attacker can no longer run arbitrary code on a device.

To totally restrict the code run on the device, code signing must also be implemented in the boot process, with the help of hardware. This is difficult to implement correctly, as shown by bugs in the implementation by Apple, Microsoft and Nintendo [48] [49] [50].

3.3.7 Vendor security posture

When security vulnerabilities are found, the reaction of the vendor greatly determines the impact. The vendor has a role to receive input on potential vulnerabilities, develop a mitigation, and update devices in the field. The vendor security posture is determined by whether the vendor has a process in place to adequately handle security issues.

The consumer mainly perceives the vendor security posture as improved communication with the vendor in relation to security. When a vendor does not provide contact information or instructions how to take action in case of reporting a security issue, it will likely not help to mitigate the issue.

Without knowledge of limitations, end users may use a device in other ways as intended by the vendor. This may result in a less secure environment. Vendors could also indicate how long the device receives security updates, and how to securely dispose or resell the device.

3.3.8 Insufficient privacy protection

Consumer devices typically store sensitive information. Devices that are deployed on a wireless network store the password of that network. Cameras can provide a video and audio recording of the home in which they are deployed. If this information were accessed by attackers, this would provide a severe privacy violation.

IoT devices and related services should handle sensitive information correctly, securely, and only after consent of the end-user of the device. This applies to both storage and distribution of sensitive information.

In case of privacy protection, the vendor plays an important role. Other than an external attacker, the vendor or an affiliated party may be responsible for a privacy breach. The vendor or service provider of an IoT device could, without explicit consent, gather information on consumer behaviour for purposes like market research. Several cases are known where IoT devices, for instance smart televisions, may be listening in on conversations within a household [51].

3.3.9 Intrusion ignorance

When a device is compromised, it often keeps functioning normally from the viewpoint of the user [27] [28]. Any additional bandwidth or power usage is usually not detected. Most devices do not have logging or alerting functionality to notify the user of any security problems. If they have, these can be overwritten or disabled when the device is hacked. The result is that users rarely discover that their device is under attack or has been compromised, preventing them from taking mitigating measures.

3.3.10 Insufficient physical security

If attackers have physical access to a device, they can open the device and attack the hardware. For example, by reading the contents of the memory components directly, any protecting software can be bypassed. Furthermore, the device may have debugging contacts, accessible after opening up the device, that provide an attacker with additional possibilities [52].

Physical attacks have impact on a single device and require physical interaction. Since it not possible to perform these attacks en-masse from the Internet, we do not recognize this as one of the biggest security problems, but it is nevertheless included.

A physical attack can be impactful if it uncovers a device key that is shared amongst all devices of the same model, and thus compromises a wide range of devices. However, in that case we consider sharing the key amongst all devices to be the more important problem (see 3.3.1), not physical security.

3.3.11 Incorrect user interaction

Vendors can encourage secure deployment of their devices by making it easy to configure them securely. By giving proper attention to usability, design, and documentation, users can be nudged into configuring secure settings [39].

There is partial overlap between this category and other categories listed above. For example, section 3.3.1 includes using unsafe or default passwords. One way to solve this is to make the user interaction with the device such that it is very easy or even mandatory to configure a secure password.

For most of the above security categories, it is difficult for a non-technical user to evaluate whether a device meets the requirement. However, user interaction can, by definition, be perceived by the end-user, and so the consumer can evaluate how well a device performs on user interaction.

User interaction is an important category to make sure implemented security measures are activated and correctly used. If it is possible to change the default password, but the user does not know or cannot discover the functionality, it is useless.

3.4 Reflection

This chapter described a threat model with two attack scenarios, as well as eleven important problems in IoT security. Comparison with found vulnerabilities and actual attacks showed that the threat model and security problems indeed apply to most attacks, giving confidence in the described model. However, the list of security problems is not meant to be exhaustive, and as such, several categories are not included in our list. For example, two problems described in the OWASP IoT top 10 are not present in our list of eleven security problems. First, our problems do not account for compromised supply chains of the vendor (item I5). We could not find sources that support an assertion that compromised supply chains are a big problem in IoT security, or demonstrate that a supply chain was compromised in an actual attack. Second, our problems are predominantly focused on the device itself, while the behaviour of surrounding systems may also have impact of the security of the device (item I3). This is a limitation of defining any scope for the security requirements; any system just outside the scope may influence the security within scope, while not bound to the requirements. A complete comparison with the OWASP IoT top 10 can be found in Appendix A .

4 Requirements analysis

4.1 Introduction

The previous chapter listed a threat model and security problems, on which we can base requirements. This chapter evaluates IoT security measures from several sources, with the goal of creating a list of specific requirements that best solve the security problems.

As described in chapter 2, Method, security measures were evaluated to produce a list of top measures to convert into basic requirements. A description of the evaluation criteria is specified in section 4.2 and the measures that were evaluated are described in section 4.3.

In the evaluation itself, each measure is judged on all criteria, and is assigned a numerical score. A description of this approach and the weights is provided in section 4.4. A variation of the scoring method is explored in section 4.5, and section 4.6 shows the scores in a graph to support choosing a cut-off point.

After ordering the measures on their evaluation score, the set of essential requirements for securing IoT devices was created by combining the top security measures. The set of essential requirements for consumer IoT is provided in section 4.7. With that, the main research question is answered: which specific security requirements are most effective in improving the security of consumer devices?

4.2 Evaluation criteria

Evaluation criteria follow from the intended use of the security requirements. Vendors need to be able to implement the security requirements in most of their products. Other parties need to be able to verify whether the requirements have been implemented, possibly without cooperation of the vendor. The requirements need to be specific, so that the vendor and other parties agree on their intended scope. Moreover, the requirements need to solve the most important security problems. This results in the following list of evaluation criteria:

- *Applicability*: requirements must be applicable to a wide range of devices and not limited to a narrow product group.
- *Specificity*: requirements must be specific, well defined and unambiguous.
- *Measurability*: it must be possible to determine whether a device objectively meets the security requirement.
- *Achievability*: it must be possible for the vendor to efficiently implement the security requirement.
- *Impact on vulnerabilities*: the requirement must resolve at least one of the most important security problems.
- *Match with threat model*: the requirement must be applicable to at least one of the attack scenarios in our threat model.

These evaluation criteria are described in detail in the following paragraphs.

4.2.1 Applicability

Applicability defines whether a measure is applicable to a wide range of devices or that the measure is specific to a limited group of devices. In general, measures that can be applied to a large group of devices are preferred. The applicability can be expressed in one of the following values:

- *Yes*: the requirement is applicable to wide range of IoT devices. The measure is not limited to a certain product group or model.
- *No*: the requirement is applicable to a limited group of IoT devices. For example, the measure is only applicable to devices that use a certain technology or have certain functionality.

4.2.2 Specificity

Specificity defines whether a measure is unambiguous and can only interpreted in one way. The specificity of measures is expressed in one of the following values:

- *Yes*: the measure is specific. Vendors can be assumed to implement the measure in an unambiguous manner.
- *No*: the measure is not specific. It is open to interpretation or too broad.

4.2.3 Measurability

Measurability defines the effort required to test fulfilment of a requirement. In general, requirements that can easily be tested are preferred. As there is a need for independent verification of requirements, measurability is qualified from two perspectives: black-box and white-box:

- Black-box is the perspective of an independent third party, a consumer or anyone who independently wants to verify the security of the device.
- White-box is the perspective of the developer or someone with full access to the device, its internals, source code and documentation.

For both perspectives, measurability is expressed in the following possible values:

- *High*: verification of the requirement is straightforward and can be done by following an instruction within approximately one hour.
- *Medium*: verification of the requirement can be done within one day and requires an experienced tester.
- *Low*: verification of the requirement requires in-depth knowledge of a certain topic (like cryptography, source code) and requires significant time (more than one day).
- *Not possible*: it is not possible to verify the requirement.

4.2.4 Achievability

Achievability defines the effort and cost for the vendor to fulfil a requirement. Requirements that can be implemented with less effort are preferred. As there is a broad range of implementation possibilities for IoT devices, making a quantitative estimation is unfeasible. Therefore, the implementation effort is qualitatively judged on aspects such as the required time, complexity and costs needed to implement the requirement compared to the state where the required functionality was not present. The following values characterize implementation effort:

- *High:* the requirement can be implemented by making a small change, such as a secure default configuration, or a trivial software change.
- *Medium:* implementation requires significant configuration or programming effort but can be realised without a major redesign of the device or architecture.

- *Low:* implementation requires a redesign of the device, or the requirement cannot be fulfilled with the current device.

4.2.5 Impact on vulnerabilities

The impact on vulnerabilities defines the result of implementation of a requirement on resolving each of the vulnerabilities or security problems listed in section 3.3. The impact of a requirement on each IoT vulnerability is expressed as the following value:

- *High*: implementation of the requirement eliminates the vulnerability or has significant contribution on resolving it.
- *Medium*: implementation of the requirement has impact on the vulnerability as it resolves some parts of the problem.
- *Low*: implementation of the requirement is related to the vulnerability, but the impact of the implantation on mitigating the vulnerability itself is small.
- *None*: implementation of the requirement has no impact on resolving the problem.

4.2.6 Impact on threat model

The impact of a requirement on an attack scenario is expressed as the requirement having a direct relation with mitigating each of the attack scenarios (*Yes*), or that a direct relation is lacking (*No*).

4.3 Sources for security measures

We used the following sets of security measures as input for the requirements analysis:

- ETSI TS 303 645 V2.1, provisions for the security of consumer devices that are connected to a network [53];
- IoT Security Compliance Framework, from the IoT Security Foundation [54];
- OWASP Internet of Things Security Verification Standard (ISVS) provides security requirements for IoT applications [55];
- ENISA Baseline security recommendations for IoT in the context of Critical Information Infrastructures [15].

As described in 2.4, these are respected and well-known lists of security measures, used in the IoT market. Together, they contain 415 security measures.

4.3.1 ETSI EN 303 645

The European Telecommunications Standards Institute (ETSI) specifies 65 security provisions for consumer IoT devices that are connected to a network [53]. The standard is meant for organisations involved in the development and manufacturing of consumer IoT devices, i.e. vendors. As such, it aims to provide a relatively complete set of requirements. In contrast, our work aims to provide a set of essential requirements that solve the most important problems. Furthermore, ETSI EN 303 645 is not constrained by measurability; in a black box test it is difficult to observe whether some provisions have been implemented. Even so, it is a quite complete and usable set of provisions, and it supports most provisions with examples and rationale.

From the wording of the provisions, it is clear ETSI wants to avoid restricting devices to a specific technology or protocol. A requirement on passwords may prevent devices from using an authentication mechanism that does not rely on passwords. Therefore, EN 303 645 uses the term "authentication value" instead of "password".

Unfortunately, in certain cases this makes the provisions insufficiently specific. An example of such a provision follows:

Provision 5.1-3 Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage.

ETSI is working on a companion report on cybersecurity assessment for consumer IoT products, but at time of preparation of this report only an early draft of this document was available.

4.3.2 IoT Security Compliance Framework

The IoT Security Foundation released the IoT Security Compliance Framework, a set of 233 requirements [54]. Requirements are either mandatory or advisory, and are applicable to certain device classes, which depend on the impact of a compromised device. However, since we have our own evaluation criteria, we did not make distinction in the compliance class or applicability of the requirements and included all in our list of potential requirements.

The framework contains many requirements that enforce a secure business process, or a secure design. Even though these are good recommendations for vendors to secure products, these are hard to test, especially from a black-box perspective. For example, 2.4.5.38, *maintenance changes should trigger full security regression testing*.

Even so, there are also many requirements that are sufficiently specific and measurable, and usable for our requirements list. For example, one of the highest scoring framework requirements is 2.4.8.4: *the product does not accept the use of null or blank passwords*.

The framework has a wide scope, and includes security requirements for mobile applications, cloud services, the supply chain and the production process. This causes several very similar requirements; passwords should be secure for the IoT device, for the mobile application, for the web interface, etc.

4.3.3 OWASP ISVS

The OWASP Internet of Things Security Verification Standard (ISVS) provides security requirements for Internet of Things (IoT) applications. It is modelled after the Application Security Verification Standard (ASVS), a standard that is growing in popularity for the verification of security controls for web-applications and web services [56].

The ISVS is currently in the very early stages of development where the latest public version is released as an appendix to the ASVS standard. It consists of a list of 34 verification requirements that are predominantly targeted at the technical security aspects of an IoT application.

In its current form, as part of the ASVS, the ISVS defines three assurance levels with increasing depth. This essentially means that an IoT application is verified against more requirements when a higher security level is selected. Level 1 requirements can be considered as the bare minimum. The requirements at this level are typically easy to verify. Level 2 introduces requirements that defend against the majority of today’s security risks. Level 3 is reserved for applications that need a high level of assurance and require significant security verification. Examples of such applications are in the area of military, health, financial or critical infrastructures.

As we have our own evaluation criteria, we did not make distinction in the assurance levels and included all in our list of potential requirements.

4.3.4 ENISA Baseline Security Recommendations for IoT

The ENISA Baseline Security Recommendations for IoT provides measures on three main categories:

- Policies
- Organisational, People and Process measures
- Technical measures

The measures regarding policies target the development process at the vendor. Virtually all of these are insufficiently SMART when applied to the end product of the process, the IoT device. The Organisational, People and Process measures target the interaction between the vendor and the consumer, and cover vulnerability disclosure, for example. Finally, the technical measures provide the most concrete measures of how the IoT device should behave.

Several of the measures that are included as a single point in the ENISA document actually consist of several requirements. For example:

GP-TM-18: Ensure that the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), that it is signed by an authorised trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins.

This one measure consists of at least eight requirements. This makes it difficult to categorize and evaluate.

The ENISA measures are meant to provide information on how to secure devices. Several measures dictate that a specific part of the device should be secure. For example:

GP-TM-35: Cryptographic keys must be securely managed.

It is self-evident that for a device to be secure, all its subcomponents need to be secure. However, for vendors that are unaware of how to develop secure components, indicating that something must be secure may be insufficient. For testers, it may even be unclear what level of security is demanded, or against what kind of attack the system should be secure. Most of these measures have been discarded as insufficiently specific.

4.4 Evaluation score

For each security measure, we determined the values for the evaluation criteria described above. For example, if a measure were easy to test, it would be marked as “high” for measurability. Subsequently, a score was assigned to each value. The score of all the criteria was added together, giving a total score for the measure. Higher scoring measures better fit the given criteria. This section briefly explains the scoring assigned to the criteria values. Appendix C provides a detailed explanation of the scoring.

Applicability, specificity, measurability and achievability were all weighted equally. Black box measurability was weighted heavier than white box measurability, since we assumed that standardisation agencies must be able to test devices without vendor cooperation. The first six problems in our list were weighted heavier than the last five problems, since we assumed these are the most important problems to solve. The scenarios from the threat model only count for a small part. Every action that secures a device has effect on both attack scenarios in some way, so which attack scenario is marked as relevant does not provide much information on the security measures.

4.5 Variation analysis

By assigning the scores as described above, a certain set of measures scored the highest and is considered the most important. The goal of the variation analysis was to investigate whether slightly modifying the scoring method results in big changes in the resulting measures. If there was a large variation when changing the scoring, this may indicate that the resulting measures are arbitrary. However, we saw that the measures remain stable when changing the scoring slightly, giving confidence that the resulting measures indeed best fitted the criteria.

To test of the variability of the scoring, a completely different method was used: knock-out criteria. For the knock-out criteria, only those measures were selected that are generally applicable, specific, measureable from a black-box perspective, are easy to implement and have a high impact on one or more security problems. Measures are not selected if they did not fit all these criteria.

Comparing the resulting list to our original list showed a large overlap as the top seventeen security measures using knock-out were the same as with the weight based scoring approach.

Nevertheless, using a knock-out based evaluation would introduce nine additional security measures. This was caused by the fact the with the knock-out criterion, the impact on each security problem is treated equally. As a result, the security problems that are at the bottom part of the list of IoT vulnerabilities (see section 3.3) become more important.

Overall we conclude that using another approach, in this case knock-out criteria instead of a weight based score, the results showed a high degree of similarity compared to when a weight based score was used, and using another approach confirms the requirements that were selected.

4.6 Scoring results

The evaluation of the, in total 415, security measures is provided in a separate spreadsheet that is added as supplement to this report. The total evaluation score of all requirements varies between 5 and 58 points. The following chart displays the evaluation scores of all measures in descending order.

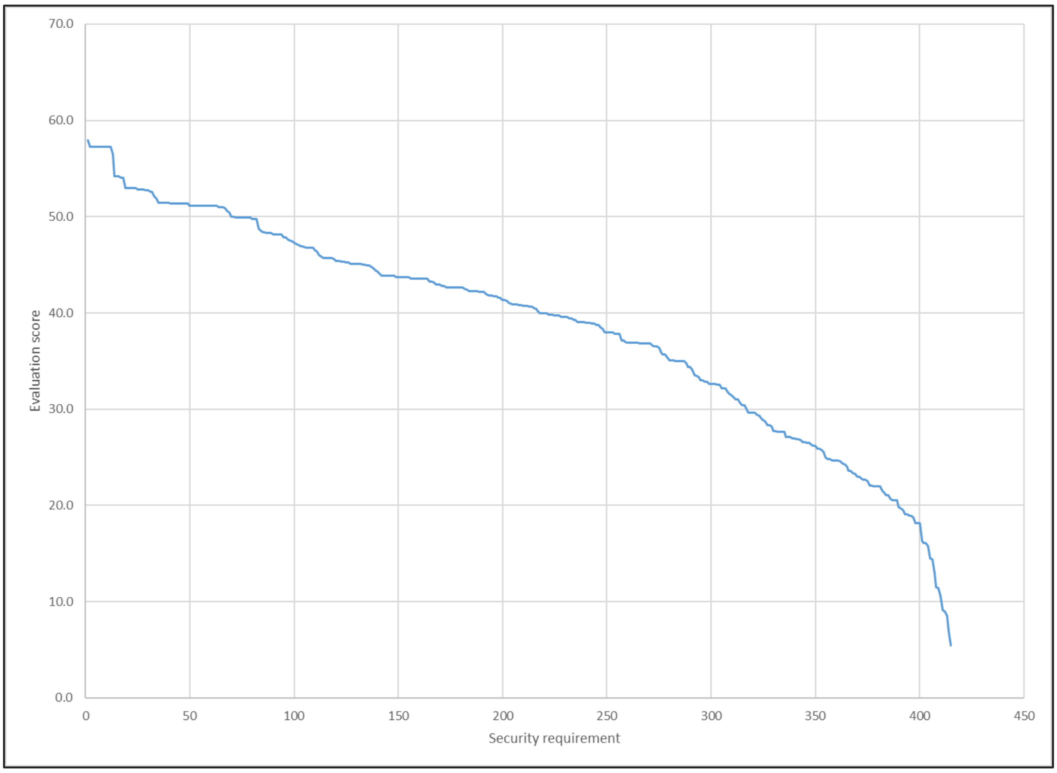


Figure 1: Requirement evaluation scores in descending order.

The following observations were made:

- After the thirteenth measure, there was a step-down in the evaluation score from above 55 to below 55. The change appears to be caused by a lower black-box measurability and lower achievability of the required functionality. After that, the evaluation score gradually decreases.
- While hardly noticeable, around the 250th measure, the evaluation score drops faster. This appears to be the result of that measures from that point were no longer judged as specific.

4.7 Essential security requirements

The set of essential requirements was established by combining the best scoring measures and converting these into a set of essential requirements. As source measures we use the first thirteen measures, before the largest drop in score is observed (see Figure 1). These requirements cover the following topics:

- passwords;
- access control;
- interfaces;
- encryption of data in transit;
- software updates;
- user privacy.

The resulting top measures (Appendix B) overlap and were inconsistently worded. We rephrase them into consistent essential security requirements. The next sections describe the source measures, the essential security requirements that follows from those measures, and explanation and rationale for the requirements.

4.7.1 Requirements for passwords

Top security measures indicate that passwords should be present, easily changeable by the user, follow a standard password policy, and should not contain the username.

The NIST SP800-63 Digital Identity Guidelines [57] offer a well-known standard password policy, which is also recommended in the IoT Security Compliance Framework. This policy dictates a minimum length and use of a blocklist to deny, for example, the username as password. Therefore, we propose the following requirement:

All passwords must conform to the industry standard NIST SP800-63b Digital Identity Guidelines.

This includes both passwords and PINs the device ship with, as the passwords that the user can configure. It applies to all used passwords, including those used for debugging or other technical purposes. Since the NIST standard dictates a minimum length, blank or empty passwords are not permitted. We feel that the standard does not impede usability in restricting passwords too much.

This requirement does not dictate that passwords must be used. Other methods of authentication may be implemented instead of passwords.

When a password is used, the NIST Digital Identity Guideline specifies: “Memorized secrets SHALL be at least 8 characters in length if chosen by the subscriber. Memorized secrets chosen randomly by the CSP or verifier SHALL be at least 6 characters in length and MAY be entirely numeric. If the CSP or verifier disallows a chosen memorized secret based on its appearance on a blacklist of compromised values, the subscriber SHALL be required to choose a different memorized secret. No other complexity requirements for memorized secrets SHOULD be imposed.”

Another top-scoring measure is that it must be possible to change passwords. The context of this is to avoid universal default passwords. We feel that the mere possibility to change passwords insufficiently solves this problem. However, the proper measures that solve this problem have a slightly lower score (42.7 instead of 45.2), because of the lower measurability: several devices are needed to compare passwords. Even so, we also considered these measures, to better formulate a requirement that solves the underlying problem:

After initial setup, passwords must be unique for each device, or defined by the user.

This requirement ensures that devices of the same model do not share the same credentials. This can be achieved by making the factory issued password unique, or by initialisation of the device. Before a device is initially configured, it is acceptable that no password is set, as long as a password is configured before the device is taken into operation.

The goal of this requirement is that the password is unique, and not easily guessable. It should therefore be avoided to derive passwords from device properties such as serial or model number.

4.7.2 Requirements for access control

Only one top security measures concerns access control:

Access to device functionality via a network interface in the initialised state must only be possible after authentication on that interface.

In other words, access control must be present. The device must only offer its functionality to an authenticated and authorised client.

The authentication is meant to identify the other party as an authorised user. Anonymous access or guest user accounts are not permitted. In addition, factory issued or OEM login accounts do not properly authenticate the user. These must be disabled, erased, or renamed before or during initial setup.

4.7.3 Requirements for interfaces

The top security measures in this category state that unused interfaces should be disabled. For example, TCP ports that offer functionality not necessary for normal operation should be disabled.

All exposed ports and interfaces must be necessary for the normal and intended use of the device.

Ports and interfaces that have a function when the device is normally used can remain available. However, ports and interfaces used for debugging during development should be disabled. In addition, an administrative interface that is meant to be available on the Wi-Fi network should not be available to the internet.

4.7.4 Requirements for encryption of data in transit

The top security measure in this category states that data in transit should be encrypted using TLS. Indeed, data in transit should be encrypted, and the parties that communicate should authenticate each other. TLS, and its datagram equivalent DTLS, are standard protocols that offer that.

All network traffic must be encrypted and authenticated using best practice encryption protocols, such as TLS.

The purpose of this requirement is to prevent other users of the same network from intercepting and manipulating traffic. This requirement allows other standard encryption protocols, such as SSH. It does not allow proprietary or custom protocols. It requires encryption both on the internet and on the local network.

This requirement focusses on having encryption of data in transit. While it is always better to further strengthen the encryption by, for instance, using the latest version of TLS, such improvements are not part of this requirement.

4.7.5 Requirements for software updates

The top security measures for software updates state that firmware updates should be performed automatically, and the authenticity and integrity of the firmware should be verified before installing.

Automatic firmware updates, in which the device updates its firmware without user interaction, are not always possible for devices that are not connected to the internet. However, in this case there should be a way of notifying the user that there is new firmware available, or at least that there is a known problem with their product.

Vendors must be able to initiate firmware updates in IoT devices, either by automatic updates or by actively informing the user about availability of updates.

Preferably, this means that firmware updates are automatically installed. If this is not technically possible without user interaction, this requirement can be fulfilled by the vendor informing the user that an update is available and should be installed. It is not acceptable to offer new firmware on the vendor's website without notifying users.

If the device has an update mechanism where the user can supply firmware, it should not be possible to supply malicious firmware. Attackers should not be able to abuse the firmware update mechanism to install malicious software. Therefore, only trusted firmware should be installed.

The device must verify the authenticity and integrity of firmware updates before installing them.

For automatic updates, this requirement is satisfied by the encryption requirement from the previous section. Having an encrypted connection with the vendor creates a trust relationship between the device and the vendor. As a result, a firmware update transferred over such a connection is implicitly trusted. However, if there is a possibility to supply a firmware image to install, it should be verified to make sure it originates from the vendor.

Both these requirements are meant to protect against attackers, and not against the end-user. It is acceptable if end users wilfully use custom firmware, or temporarily deny an update, if they are aware of the risk.

4.7.6 Requirements for user privacy

The top security measure in this category states that the vendor needs to inform the user about how to achieve security and privacy. Security and privacy issues can arise if a device is incorrectly used. For example, connecting a camera to the internet instead of to a private network can have large privacy implications. If the user needs to configure the device in a secure way, that should be made clear.

The vendor must provide clear and understandable information about the end user's responsibilities to set up and maintain the device's privacy and security.

This requirement makes it possible to assign responsibility for securely configuring the device to either the vendor or the end user. It is not sufficient that it is possible to configure a device securely as both the vendor and the user may leave that functionality unused.

Preferably, the vendor should take responsibility for securing the device. In reality, there are limitations to the environments in which devices can be reasonable secure. A baby monitor is not sufficiently secure to guard a bank vault. It is up to the vendor to inform the consumer of the limitations of their product, and the responsibilities of the consumer.

4.8 Summary

The following basic requirements were described:

- All passwords must conform to the industry standard NIST SP800-63b Digital Identity Guidelines.
- After initial setup, passwords must be unique for each device, or defined by the user.
- Access to device functionality via a network interface in the initialised state must only be possible after authentication on that interface.
- All exposed ports and interfaces must be necessary for the normal and intended use of the device.
- All network traffic must be encrypted and authenticated using best practice encryption protocols, such as TLS.
- Vendors must be able to initiate firmware updates in IoT devices, either by automatic updates or by actively informing the user about availability of updates.
- The device must verify the authenticity and integrity of firmware updates before installing them.
- The vendor must provide clear and understandable information about the end user’s responsibilities to set up and maintain the device’s privacy and security.

5 Conclusion and recommendations

Attacks on IoT devices are typically not very sophisticated. Using default credentials or connecting to an open port can be sufficient to compromise a device. Many devices are lacking even basic security measures. Therefore, a relatively small set of requirements can already have a large effect on the security of products. The proposed essential security requirements do not solve all IoT security problems described in chapter 3, but they provide a realistic first step to greatly improve consumer IoT security.

More than 400 security measures were evaluated, ultimately resulting in a set of essential security requirements for consumer IoT devices in five categories. Only those measures that are specific and effective in improving the security of consumers were selected for the set of essential security requirements. The set of requirements will help standardisation bodies in their effort to arrive at a well-weighted and substantiated set of requirements for a standard framework for cyber-safe IoT equipment.

Both cybersecurity and IoT are fields where rapid developments take place. We recommend that these essential requirements be periodically evaluated. New best practices in cybersecurity or new developments on consumer IoT may call for fine-tuning of the requirements.

We evaluated several sources of requirements. Only a subset of these requirements was useful for our purpose. Many requirements were eliminated because they were not specific enough. Several requirements specified that a component should be secured, but not how to achieve that. Requirements were also eliminated when it was impossible to test whether a device meets the requirement from a black box perspective. Furthermore, the requirements aim to completely secure devices from many attack vectors, while we attempted to provide a set of requirements to protect against the worst attacks. We recommend that organisations that compose security requirements make them specific, testable, and clearly indicate the security benefit a requirement provides.

Of course, it is the ultimate purpose of this report that IoT devices comply with the proposed requirements. We recommend vendors implement security in a way that is easy to use for the consumer, and openly communicate about the security measures in their product. This includes accepting feedback from consumers and vulnerability reports from security researchers in the context of coordinated vulnerability disclosure (CVD).

This work is primarily focussed on securing IoT devices. However, these devices are used in home networks and are typically connected through the Internet to web applications, mobile apps and back-end services. Further research could propose methods to improve the security of the whole ecosystem.

6 Glossary

Term	Definition
ASVS	Application Security Verification Standard
CEN	Comité Européen de Normalisation, European Committee for Standardization
CENELEC	Comité Européen de Normalisation Electrotechnique
CVD	Coordinated Vulnerability Disclosure
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
DVB-T	Digital Video Broadcasting — Terrestrial
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
HTTP	Hypertext Transfer Protocol
IoT	Internet-of-Things
ISVS	IoT Security Verification Standard
MitM	Man-in-the-Middle
OWASP	Open Web Application Security Project, an open source foundation for application security
RED	Radio Equipment Directive
SMART	Criteria to guide in the setting of objectives that are Specific, Measurable, Achievable, Relevant and Time-bound.
SSH	Secure Shell
SSL	Secure Sockets Layer, a deprecated encrypted protocol, replaced by TLS.
TCP	Transmission Control Protocol
TLS	Transport Layer Security, an encrypted protocol that replaces SSL.
TV	Television

Table 2: Terms and abbreviations.

7 Bibliography

[1] Radiocommunications Agency Netherlands, “Onveilige apparatuur risico voor samenleving,” *Staat van de Ether,* 2017.

[2] Radiocommunications Agency Netherlands, “Veilig verbonden apparaten,” *Staat van de Ether,* 2019.

[3] Strict B.V., “Rapport over de digitale veiligheid van IoT-apparatuur,” 2019. [Online]. Available: https://www.agentschaptelecom.nl/documenten/rapporten/2019/09/25/rapport-digitale-veiligheid-van-iot-apparatuur.

[4] O. Alrawi, C. Lever, M. Antonakakis and F. Monrose, “Sok: Security evaluation of home-based iot deployments,” in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019.

[5] H. A. Abdul-Ghani and D. Konstantas, “A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective,” *Journal of Sensor and Actuator Networks,* vol. 8, p. 22, April 2019.

[6] J. Saleem, M. Hammoudeh, U. Raza, B. Adebisi and R. Ande, “IoT standardisation,” in *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems - ICFNDS 18*, 2018.

[7] M. R. Warner, C. Gardner, R. Wyden and S. Daines, “Internet of Things (IoT) Cybersecurity Improvement Act of 2017,” in *Proc. 115th U.S. Congress*, 2017.

[8] M. Warman, “Consultation on regulatory proposals on consumer IoT security,” 2020.

[9] European Parliament, “Directive 2014/53/EU of the European Parliament and of the Council,” *Official Journal of the European Union,* 2014.

[10] A. A. Gendreau and M. Moorman, “Survey of intrusion detection systems towards an end to end secure internet of things,” in *2016 IEEE 4th international conference on future internet of things and cloud (FiCloud)*, 2016.

[11] B. B. Zarpelão, R. S. Miani, C. T. Kawakani and S. C. de Alvarenga, “A survey of intrusion detection in Internet of Things,” *Journal of Network and Computer Applications,* vol. 84, p. 25–37, 2017.

[12] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz and J. Lopez, “A Survey of IoT-Enabled Cyberattacks: Assessing Attack Paths to Critical Infrastructures and Services,” *IEEE Communications Surveys & Tutorials,* vol. 20, p. 3453–3495, 2018.

[13] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford and V. Sivaraman, “Systematically Evaluating Security and Privacy for Consumer IoT Devices,” in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy - IoTS&P '17*, 2017.

[14] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum and N. Ghani, “Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations,” *IEEE Communications Surveys Tutorials,* vol. 21, pp. 2702-2733, 2019.

[15] ENISA, “Baseline security recommendations for IoT in the context of Critical Information Infrastructures,” 2017.

[16] N. Zhang, S. Demetriou, X. Mi, W. Diao, K. Yuan, P. Zong, F. Qian, X. Wang, K. Chen, Y. Tian, C. A. Gunter, K. Zhang, P. Tague and Y.-H. Lin, “Understanding IoT Security Through the Data Crystal Ball: Where We Are Now and Where We Are Going to Be,” 28 March 2017.

[17] M. Frustaci, P. Pace, G. Aloi and G. Fortino, “Evaluating Critical Security Issues of the IoT World: Present and Future Challenges,” *IEEE Internet of Things Journal,* vol. 5, p. 2483–2495, August 2018.

[18] P. Emami-Naeini, Y. Agarwal and L. F. Cranor, “Specification for an IoT Privacy and Security Label,” 2020.

[19] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis and others, “Understanding the mirai botnet,” in *26th USENIX Security Symposium (USENIX Security 17)*, 2017.

[20] A. Jha and M. C. Sunil, “Security considerations for Internet of Things,” *L&T Technology Services,* 2014.

[21] M. Hogan, B. Piccarreta, I. I. C. S. W. Group and others, “Interagency report on status of international cybersecurity standardization for the Internet of Things (IoT),” 2018.

[22] J. Bugeja, D. Jonsson and A. Jacobsson, “An Investigation of Vulnerabilities in Smart Connected Cameras,” in *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 2018.

[23] A. Chapman, “Hacking into Internet Connected Light Bulbs,” Context, 2014. [Online]. Available: https://www.contextis.com/us/blog/hacking-into-internet-connected-light-bulbs.

[24] N. Apthorpe, D. Reisman and N. Feamster, “A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic,” 18 May 2017.

[25] J. Margolis, T. Oh, S. Jadhav, J. Jeong, Y. H. Kim and J. N. Kim, “Analysis and Impact of IoT Malware,” in *Proceedings of the 18th Annual Conference on Information Technology Education - SIGITE '17*, 2017.

[26] M. Kumar, “Cyber Attack Knocks Nearly a Million Routers Offline,” The Hacker News, 2016. [Online]. Available: https://thehackernews.com/2016/11/mirai-router-offline.html.

[27] C. McDermott, J. Isaacs and A. Petrovski, “Evaluating Awareness and Perception of Botnet Activity within Consumer Internet-of-Things (IoT) Networks,” *Informatics,* vol. 6, p. 8, February 2019.

[28] K. Angrishi, “Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets,” 13 February 2017.

[29] G. Kambourakis, C. Kolias and A. Stavrou, “The Mirai botnet and the IoT Zombie Armies,” in *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, 2017.

[30] S. Soltan, P. Mittal and H. V. Poor, “BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid,” in *27th USENIX Security Symposium (USENIX Security 18)*, Baltimore, 2018.

[31] de Volkskrant, “Ict-lek zonnepanelen mogelijk bedreigend voor Europese stroomvoorziening,” 4 August 2017. [Online]. Available: https://www.volkskrant.nl/nieuws-achtergrond/ict-lek-zonnepanelen-mogelijk-bedreigend-voor-europese-stroomvoorziening~bef49c64/. [Accessed 26 June 2020].

[32] C. Williams, “RISK: Is This Your Webcam? You’re Being Watched,” WizCase, 2019. [Online]. Available: https://www.wizcase.com/blog/webcam-security-research/.

[33] P. Kulche, “Beveiligingscamera’s blijken onveilig,” Consumentenbond, 2019. [Online]. Available: https://www.consumentenbond.nl/beveiligingscamera/beveiligingscameras-onveilig.

[34] E. Fernandes, J. Jung and A. Prakash, “Security Analysis of Emerging Smart Home Applications,” in *2016 IEEE Symposium on Security and Privacy (SP)*, 2016.

[35] D. Fisher, “What’s on TV Tonight? Ransomware,” Pindrop, 2016. [Online]. Available: https://www.pindrop.com/blog/whats-on-tv-tonight-ransomware/.

[36] C. Wueest, “How my TV got infected with ransomware and what you can learn from it,” *Broadcom Community,* 2015.

[37] R. Scheel, “Smart TV Hacking (Video: Oneconsult Talk at EBU Media Cyber Security Seminar),” 2017. [Online]. Available: https://www.oneconsult.com/en/smart-tv-hacking/.

[38] T. Beardsley, “IoT Vuln Disclosure: Children's GPS Smart Watches (R7-2019-57),” Rapid7, 2019. [Online]. Available: https://blog.rapid7.com/2019/12/11/iot-vuln-disclosure-childrens-gps-smart-watches-r7-2019-57/.

[39] B. Ur, J. Jung and S. Schechter, “The current state of access control for smart devices in homes,” in *Workshop on Home Usable Privacy and Security (HUPS)*, 2013.

[40] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu and X. Fu, “Security vulnerabilities of internet of things: A case study of the smart plug system,” *IEEE Internet of Things Journal,* vol. 4, p. 1899–1909, 2017.

[41] Y. Yao, W. Zhou, Y. Jia, L. Zhu, P. Liu and Y. Zhang, “Identifying Privilege Separation Vulnerabilities in IoT Firmware with Symbolic Execution,” in *European Symposium on Research in Computer Security*, 2019.

[42] T. H.-J. Kim, L. Bauer, J. Newsome, A. Perrig and J. Walker, “Access right assignment mechanisms for secure home networks,” *Journal of Communications and Networks,* vol. 13, p. 175–186, April 2011.

[43] C. Cimpanu, “Two botnets are fighting over control of thousands of unsecured Android devices,” ZDNet, 2018. [Online]. Available: https://www.zdnet.com/article/two-botnets-are-fighting-over-control-of-thousands-of-unsecured-android-devices/.

[44] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman and R. Boreli, “An experimental study of security and privacy risks with emerging household appliances,” in *2014 IEEE Conference on Communications and Network Security*, 2014.

[45] Technology.org, “Update: Symantec discovers Linux.Darlloz worm targetting embedded systems,” 2013. [Online]. Available: https://www.technology.org/2013/12/03/update-symantec-discovers-linux-darlloz-worm-targetting-embedded-systems/.

[46] M. Shobana and S. Rathi, “IOT Malware: An Analysis of IOT Device Hijacking,” *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* 2018.

[47] B. Botezatu, “Remote Exploitation of the NeoCoolcam IP Cameras and Gateway,” Bitdefender, 2017. [Online]. Available: https://labs.bitdefender.com/2017/08/remote-exploitation-of-the-neocoolcam-ip-cameras-and-gateway/.

[48] Kim Jong Cracks, “checkra1n,” 2019. [Online]. Available: https://checkra.in/.

[49] A. Huang, Hacking The Xbox, No Starch Press,US, 2003.

[50] noahc3, "The Ultimate Noob Guide for Hacking your Nintendo Switch," 2019. [Online]. Available: https://switch.homebrew.guide/.

[51] M. Rotenberg, J. Horwitz and A. Butler, "EPIC Letter to the Attorney General and the FTC Chairwoman," 10 July 2015. [Online]. Available: https://epic.org/privacy/internet/ftc/EPIC-Letter-FTC-AG-Always-On.pdf. [Accessed 26 June 2020].

[52] S. Vasile, D. Oswald and T. Chothia, "Breaking All the Things—A Systematic Survey of Firmware Extraction Techniques for IoT Devices," in *Smart Card Research and Advanced Applications*, Cham, 2019.

[53] ETSI, "EN 303 645 - Cyber Security for Consumer Internet of Things," 2019.

[54] IoT Security Foundation, "IoT Security Compliance Framework," 2020.

[55] The OWASP IoT Security Team, "OWASP IoT Security Verification Standard ISVS," 2019. [Online]. Available: https://github.com/OWASP/IoT-Security-Verification-Standard-ISVS. [Accessed 25 June 2020].

[56] The OWASP Foundation, "Application Security Verification Standard 4.0," March 2019. [Online]. Available: https://github.com/OWASP/ASVS/raw/master/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0-en.pdf. [Accessed 26 June 2020].

[57] P. A. Grassi, M. E. Garcia and J. L. Fenton, "NIST Special Publication 800-63-3 Digital Identity Guidelines," *National Institute of Standards and Technology, Los Altos, CA,* 2017.

[58] The OWASP IoT Security Team, "Internet of Things (IoT) Top 10 2018," 2018. [Online]. Available: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf. [Accessed 25 June 2020].

[59] T. Yu, V. Sekar, S. Seshan, Y. Agarwal and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks - HotNets-XIV*, 2015.

[60] A. Sivanathan, D. Sherratt, H. H. Gharakheili, V. Sivaraman and A. Vishwanath, "Low-cost flow-based security solutions for smart-home IoT devices," in *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2016.

[61] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017.

[62] J. Bugeja, A. Jacobsson and P. Davidsson, "On privacy and security challenges in smart connected homes," in *2016 European Intelligence and Security Informatics Conference (EISIC)*, 2016.

[63] E. Bou-Harb and N. Neshenko, Cyber Threat Intelligence for the Internet of Things, Springer International Publishing, 2020.

[64] J. E. Kim, G. Boulos, J. Yackovich, T. Barth, C. Beckel and D. Mosse, "Seamless Integration of Heterogeneous Devices and Access Control in Smart Homes," in *2012 Eighth International Conference on Intelligent Environments*, 2012.

[65] K. Yang, D. Forte and M. M. Tehranipoor, "Protecting endpoint devices in IoT supply chain," in *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2015.

[66] M. Fagan, K. Megas, K. Scarfone and M. Smith, “NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers,” May 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf.

[67] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari and H. Karimipour, “A survey on internet of things security: Requirements, challenges, and solutions,” *Internet of Things,* p. 100129, 2019.

[68] F. A. Alaba, M. Othman, I. A. T. Hashem and F. Alotaibi, “Internet of Things security: A survey,” *Journal of Network and Computer Applications,* vol. 88, p. 10–28, June 2017.

[69] D. E. Kouicem, A. Bouabdallah and H. Lakhlef, “Internet of things security: A top-down survey,” *Computer Networks,* vol. 141, p. 199–221, August 2018.

[70] H. Lin and N. Bergmann, “IoT Privacy and Security Challenges for Smart Home Environments,” *Information,* vol. 7, p. 44, July 2016.

[71] P. N. Railkar, P. N. Mahalle, G. R. Shinde and H. R. Bhapkar, “Threat analysis and attack modeling for machine-to-machine communication toward Internet of things,” *The Internet of Everything: Advances, Challenges and Applications,* pp. 45-72, 30 August 2019.

Appendices

Appendix A Comparison with OWASP IoT top 10

We compared the list of eleven most important security problems with the OWASP IoT Top 10 [58], a list of the highest priority issues for manufacturers, enterprises, and consumers.

Neither list aims to be exhaustive, so no complete mapping can be expected. Even so, the OWASP IoT Top 10 maps well with our categories. Differences in categorisation mainly arise when the IoT Top 10 defines a security problem in a subcomponent, without specifying the specifics of the security problem. Overall, the mapping gives confidence in our problem categorisation. The mapping surfaced two points of attention. First, our list of eleven security problems do not account for compromised supply chains of the vendor (item I5). Second, our problems are predominantly focused on the device itself, while the behaviour of surrounding systems may also have impact of the security of the device (item I3).

I1: Weak, guessable, or hardcoded passwords

Unsafe credentials that grant unauthorised access corresponds to the problem of incorrect access control. Both the OWASP IoT Top 10 and this work have this problem at the top position, emphasizing the importance of this problem. The category of incorrect access control is broader than password usage alone, since it also includes total lack of authentication, and incorrect authorisation.

I2: Insecure network services

This issue mentions two problems: unneeded network services and insecure network services. Unneeded network services are covered by overly large attack surface. Again, this is at number two in both lists, supporting the problem priority.

Even though insecure network services cannot be clearly mapped to a problem described above, this can be attributed to the tautology of defining security in terms of itself. When something is insecure, it is a security problem. The proposed categorization aims to be more specific as to what makes the service insecure.

I3: Insecure ecosystem interfaces

Again, this defines a security problem in terms of itself. However, it correctly points out that securing the device is only a partial solution if the corresponding cloud service or mobile app is not well secured. This is a limitation of defining any scope for the security requirements; any system just outside the scope may influence the security within scope, while not bound to the requirements.

OWASP provides several examples of this issue: lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering. These correspond to our categories of incorrect access control, lack of encryption, and application vulnerabilities.

I4: Lack of secure update mechanism

Lack of any update mechanism is covered by the issue outdated software. This OWASP issue also includes authentication of the firmware, to only install trusted and up-to-date firmware. This maps to our problem of a lack of trusted execution environment.

I5: Use of insecure or outdated components

Use of outdated components is included in the issue of outdated software. According to OWASP, this includes using software or hardware from a compromised supply chain. Even though we have included a category for outdated software as an important security problem, there is no separate category for a compromised supply chain. However, we could not find sources that support that compromised supply chains are an important problem in IoT security.

I6: Insufficient privacy protection

This issue has been included in our set of security problems. Both in the top 10 and our work, this concerns how sensitive information is stored and handled on the device. The top 10 also includes the ecosystem around the device, but that is out of scope for our aim.

I7: Insecure data transfer and storage

This can be mapped to lack of encryption and insufficient access control.

I8: Lack of device management

This includes security support and update management, which we included under outdated software. Monitoring security issues and properly responding to them is part of the vendor security posture.

I9: Insecure default settings

This maps partially to user interaction: it must be easy for the user to configure the device securely. Furthermore, a specific issue may map to a category, depending on the effect of the setting. Insecure default passwords can be mapped to incorrect access control. Insecure firewall settings to overly large attack surface.

I10: Lack of physical hardening

This corresponds to the problem of deficient physical security. OWASP correctly points out that a physical attack on one device can help in a future remote attack on other devices. Therefore, even though physical attacks do not directly conform to our threat scenarios, physical security may provide defence-in-depth to a multi-stage attack. A physical attack on one device may provide a key, password, or other information that can be used to attack other devices.

Appendix B Relevant source security measures

This chapter lists high-scoring measures across problem categories. Further information on all measures can be found in the attached spreadsheet: AGENT-2001-06.103.

Requirements for passwords

An overview of the requirements that are selected as input for authenticator requirements is provided in the following table:

Source	Id	Requirement
ETSI EN 303 645 V2.1.0	Provision 5.1-4	Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.
IoTSF Security Compliance Framework Release 2.1	2.4.8.4	The product does not accept the use of null or blank passwords.
IoTSF Security Compliance Framework Release 2.1	2.4.10.17	Password entry follows industry standard practice such recommendations of the 3GPP TS33.117 Password policy. [ref. 17] or NIST SP800-63b [ref 26]
IoTSF Security Compliance Framework Release 2.1	2.4.11.2	Password entry follows industry standard practice such recommendations of the 3GPP TS33.117 Password policy. [ref. 17] or NIST SP800-63b [ref 26]
IoTSF Security Compliance Framework Release 2.1	2.4.8.5	The product will not allow new passwords containing the user account name with which the user account is associated.
IoTSF Security Compliance Framework Release 2.1	2.4.8.6	Password entry follows industry standard practice such recommendations of the 3GPP TS33.117 Password policy. [ref. 17] or NIST SP800-63b Digital Identity Guidelines - Authentication and Lifecycle Management" [ref 26] or NCSC [Ref 48] on password length, characters from the groupings and special characters.

Table 3: Source requirements for passwords.

Requirements for access control

An overview of the requirements that are selected on the topic of access control are provided in the following table:

Source	Id	Requirement
ETSI EN 303 645 V2.1.0	Provision 5.5-4	Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.

Table 4: Source requirements for access control.

Requirements for interfaces

An overview of the requirements that are selected on the topic of interfaces are provided in the following table:

Source	Id	Requirement
ENISA	GP-TM-50	Ensure only necessary ports are exposed and available.
ETSI EN 303 645 V2.1.0	Provision 5.6-1	All unused network and logical interfaces shall be disabled.

Table 5: Source requirements for interfaces.

Requirements for encryption of data in transit

An overview of the requirements that are selected on the topic of encryption of data in transit are provided in the following table:

Source	Id	Requirement
OWASP ASVS Appendix C	C.7	Verify that the firmware apps protect data-in-transit using transport layer security.

Table 6: Source requirements for data transit.

Requirements for software updates

An overview of the requirements that are selected on the topic of software updates are provided in the following table:

Source	Id	Requirement
ETSI EN 303 645 V2.1.0	Provision 5.3-9	The device should verify the authenticity and integrity of software updates.
ETSI EN 303 645 V2.1.0	Provision 5.3-4	Automatic mechanisms should be used for software updates.

Table 7: Source requirements for software updates.

Requirements for user privacy

An overview of the requirements that are selected on the topic of user privacy are provided in the following table:

Source		
IoTSF Security Compliance Framework Release 2.1	2.4.12.12	The supplier or manufacturer of any devices or services shall provide clear information about the end user's responsibilities to maintain the devices and/or services privacy and security.

Table 8: Source requirements for user privacy.

Appendix C Detailed evaluation scoring

After scoring/evaluating each requirement on the evaluation criteria, an evaluation score is calculated as the sum of weighted scores on each evaluation criterion. This section describes the rationale behind the calculation of the evaluation score and the weights assign to each evaluation criterion.

The evaluation score is defined as the sum of the score for each individual criterion, where the individual is expressed as a percentage. The initial assumption, and at first sight most logical, is to give each criterion the same weight. As a requirement typically (not always) resolves one or two security vulnerabilities, the weight of 'impact on vulnerabilities' in the total evaluation score is effectively lower. Therefore, the weight of this criterion is increased so that the evaluation score is similar to the score for measurability. Another adjustment is made for the weight for the impact on security threats. As the relation between the requirement and the attack scenario is less clear, the weight is reduced (halved) in comparison with the other criteria. An overview of the weights for each criterion is provided in the following table:

Criterion	Weight
Applicability	12.1%
Specificity	12.1%
Measurability (black and white box)	12.1%
Achievability	12.1%
Impact on vulnerabilities (11 vulnerabilities)	48.5%
Impact on threat model (2 attack scenarios)	3%

Table 9: Distribution of weights.

The impact on vulnerabilities or security problems is configured in such a way that more weight is assigned to the most important vulnerabilities, those with the highest security risk. The rationale used in assigning the weights is to minimise differentiation between vulnerabilities as their position may vary. Therefore, a weight is assigned to the top six vulnerabilities which twice the weight of the other vulnerabilities. An overview of the weights used for each vulnerability is provided in the following table:

Vulnerability	Weight
Incorrect access control	12%
Overly large attack surface	12%
Outdated software	12%
Lack of encryption	12%
Application vulnerabilities	12%
Lack of trusted execution environment	12%
Vendor security posture	6%
Insufficient privacy protection	6%
Intrusion ignorance	6%
Deficient physical security	6%
User interaction	6%

Table 10: Weight distribution of vulnerabilities.

Both attack scenarios of the threat model are given an equal weight (each 50%). As the preferred testing approach for measurability is a black-box perspective, it is assigned a weight of 70% and white-box 30%.

For evaluation criteria, like applicability, specificity, and impact on attack scenarios, the possible values are Yes (passes the evaluation) and No (evaluation fails). 100% (of the weight for that criterion) is assigned to the evaluation score in case of Yes, and 0% otherwise.

For the criteria measurability, achievability and impact on vulnerabilities, the outcome is expressed on a scale that varies between Not possible (or No) and High, a high degree of fulfilling the evaluation criterion. The weights of each outcome is provided in the following table:

Measurability	Weight
High	100%
Medium	50%
Low	25%
Not possible	0%

Table 11: Weights for measurability.

A complete overview of all weights for each evaluation criterion is provided in the following table. The score (fourth column) is calculated by multiplying the weights for the evaluation criterion, category and value. The scores are rounded to the nearest tenth.

Criterion		Value	Score
Applicability (12.1%)		Yes (100%)	12.1%
		No (0%)	0.0%
Specificity (12.1%)		Yes (100%)	12.1%
		No (0%)	0.0%
Measurability (12.1%)	Black-box (70%)	High (100%)	8.5%
		Medium (50%)	4.2%
		Low (25%)	2.1%
		No (0%)	0.0%
	White-Box (30%)	High (100%)	3.6%
		Medium (50%)	1.8%
		Low (25%)	0.9%
		No (0%)	0.0%
Achievability (12.1%)		High (100%)	12.1%
		Medium (50%)	6.1%
		Low (25%)	3.0%
		No (0%)	0.0%
Impact on vulnerabilities (48.5%)	Insufficient Access Control, Overly large attack surface, Outdated software, lack of encryption, Application vulnerabilities, Lack of trusted execution environment (each 12%)	High (100%)	5.7%
		Medium (50%)	2.9%
		Low (25%)	1.4%

		None (0%)	0.0%
	Vendor security posture, Insufficient privacy protection, Intrusion Ignorance, Deficient Physical Security, User interaction (each 6%)	High (100%)	2.9%
		Medium (50%)	1.4%
		Low (25%)	0.7%
		None (0%)	0.0%
Impact on threats (3.0%)	Home IoT used as an amplifier (50%)	Yes (100%)	1.5%
		No (0%)	0.0%
	Home IoT used as a target (50%)	Yes (100%)	1.5%
		No (0%)	0.0%

Table 12: Overview of weights.