Report on
IoT Device Security

Colophon

Document name	Report on IoT Device Security v1.3
Title	Report on IoT Device Security
Reference	Agentschap Telecom, 'Onderzoek veiligheid apparaten', kenmerk 201901072, 15-02-2019
Version and date	V1.3, 16/9/19
Author	Strict B.V.
Department	Cybersecurity Solutions and Advice
Project	201902-4830 AT - TN177713
Contact details	**Strict** Lange Dreef 11-f, 4131 NJ Vianen Postbus 12, 4130 EA Vianen T. 088 55 55 800 + info@strict.nl + www.strict.nl

Version control

Date	Status	Version	Author	Description
12/09/2019	Final	1.3	Strict	Update after manufacturer review.
28/08/2019	Final	1.2	Strict	Update after manufacturer review.
26/08/2019	Final	1.1	Strict	Update after manufacturer review.
21/05/2019	Final	1.0	Strict	Final version completed.
17/05/2019	Pre-final	0.9	Strict	Document finalized, pending review.
03/05/2019	Draft	0.5	Strict	Draft version completed.
22/04/2019	Initial	0.1	Strict	Document outline.

CONTENTS

MANAGEMENTSAMENVATTING

Het ‘Internet of Things’ (IoT) groeit snel. Er wordt geschat dat eind 2021 zo’n 25 miljard IoT-apparaten in gebruik zullen zijn, tegen 14 miljard eind 2019. Deze apparaten zijn ontwikkeld met het oog op nieuwe functionaliteit, waarbij beveiliging en privacy relatief weinig aandacht krijgen: vele voorbeelden zijn bekend van beveiligingsincidenten die veroorzaakt zijn door onveilige IoT-apparaten.

Om inzicht te krijgen in de huidige staat van de beveiliging van IoT-consumentenapparaten heeft Agentschap Telecom onderzoek laten verrichten naar de digitale beveiliging van deze apparatuur op de Nederlandse markt. Agentschap Telecom kan dit rapport gebruiken als referentie bij het opstellen van Nederlandse standaarden en ondersteunende richtlijnen voor IoT-consumentenapparaten.

Dit rapport bevat de resultaten van onderzoek naar de veiligheid van 22 IoT-consumentenapparaten, te weten internet routers, connected toys, IP camera’s, slimme sloten, babyfoons en slimme thermostaten. In het onderzoek is gekeken in hoeverre de software van de apparaten voldoet aan de principes van ‘Security by Design’, ‘Security by Default’, ‘Privacy by Design’ en ‘Privacy by Default’. Dit is gedaan door een scan uit te voeren op kwetsbaarheden in de software en de standaardconfiguratie, en te kijken naar de communicatiestromen. Tevens is onderzocht welke gegevens de apparaten verzamelen, hoe deze opgeslagen worden en hoe de leveranciers volgens hun privacy statements met deze gegevens omgaan. Waar mogelijk zijn concrete aanbevelingen gegeven voor verbeteringen.

Uit het onderzoek is gebleken dat vier van de 22 apparaten bevindingen hadden die als 'kritiek' werden geclassificeerd. Respectievelijk vier en negen van de apparaten hadden bevindingen waarvan de ernst 'hoog' of 'medium' was. Voor slechts twee van de apparaten hadden we helemaal geen bevindingen.

Versleuteling en informatie-uitwisseling zijn onderdelen die nog verder verbeterd moeten worden, in het bijzonder waar de verwerking van persoonsgegevens plaatsvindt. Verbeteringen zijn ook nodig bij het oplossen van kwetsbaarheden door middel van (automatische) software-updates, aangezien dit in meerdere gevallen niet veilig ingericht is. Verder zijn er bij verschillende apparaten onnodige en onveilige services aangetroffen, dit behoeft ook extra aandacht. In het onderzoek scoren met name connected toys en babyfoons slechter op het gebied van veiligheid.

EXECUTIVE SUMMARY

The 'Internet of Things' (IoT) is growing rapidly. It is expected that a total of 25 billion IoT devices will be in use by the end of 2021, up from 14 billion in 2019. These products are developed with new functionality in mind, while security and privacy are not necessarily a priority: numerous examples exist of security breaches caused by insecure IoT devices.

In order to gain insight into the current state of IoT device security, Radiocommunications Agency Netherlands commissioned research into the digital security of these devices on the Dutch consumer market. Radiocommunications Agency Netherlands can use this report as a reference when drawing up standards and supporting guidelines for IoT consumer devices for the Dutch market.

This report contains the research results of 22 IoT consumer devices, namely internet routers, connected toys, IP cameras, smart locks, baby monitors and smart thermostats. The study investigates to what extent the software of these devices adheres to the principles of 'Security by Design', 'Security by Default', 'Privacy by Design' and 'Privacy by Default'. This was done by performing a scan for vulnerabilities in the software, analyzing the standard configuration and looking at the communication flows. Further, investigation was done to check which data the devices collect, how the data is stored and how the suppliers handle this data, according to their privacy statements. Where possible, concrete recommendations have been given for improvements.

In general, we found that four of the 22 devices had findings that were classified as 'critical'. Respectively four and nine of the devices had findings of which the severity was 'high' or 'medium'. Only for two of the devices we did not have any findings at all.

Our findings show that encryption and information exchange are areas that still need improvement, especially when personal data is transferred. Further improvements are also needed when resolving vulnerabilities through (automatic) software updates, as the update processes are often implemented insecurely. Moreover, in several cases insecure and unneeded services were encountered. This also leaves room for improvement. Our research indicated that connected toys and baby monitors are more insecure than other researched devices.

1 INTRODUCTION

The 'Internet of Things' (IoT) is growing rapidly. It is expected that a total of 25 billion IoT devices will be in use by the end of 2021, up from 14 billion in 2019[1]. It is changing the way people work, live, play and learn and it will transform our daily lives and the world as we know it today. IoT allows users to work from anywhere at any time. It allows house owners to look who is ringing their doorbell while they are abroad. And it teaches our children the names of animals using educative applications while playing with connected toys.

Manufacturers are constantly pushed to quickly deliver new IoT products to the market. These products are developed with new functionality in mind and security is in general not a priority. Numerous examples exist of security breaches caused by insecure IoT devices. Examples include network breaches through temperature sensors in an aquarium and recordings made with children's toys which are stored on publicly accessible servers. There have been a lot of smart lock security issues in the past[2][3].

As IoT devices are more widely deployed, a wide range of social, legal and ethical issues arise. These issues include ownership of data, security improvements and regulatory protections such as compliance with the General Data Protection Regulation (GDPR) and the ePrivacy directive.

IoT devices are connected through the internet. When the data contains personal information from consumers, privacy is at risk. For example, a smart thermostat can detect when residents are home. This is information criminals can use to determine the proper times to break in without being disturbed. As another example, many IoT devices have cameras or microphones that are always collecting data, and often this data is processed by third parties. Even without considering malicious parties co-opting these devices, collecting and processing this data can cause all sorts of privacy issues.

In order to assess the level of security of IoT consumer devices, a security assessment was conducted. This report describes the results of said assessment, performed on a total of 22 IoT devices available to Dutch consumers. The devices are categorized as follows:

- **Internet WiFi modems/routers.** Devices that enable consumers to create and manage their own private network, create wireless access points, and generally enable internet access for devices within their homes.
- **Connected toys.** Toys, often marketed to children, which have some electronic component that allows them to react to, or be controlled by, the user. Connected toys often are controlled using

[1] As forecasted by Gartner: https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends (last viewed on May 15th, 2019)
[2] DEFCON 24, Backdooring the Frontdoor
[3] HITBSecConf2017, Blue Picking – Hacking Bluetooth Smart Locks

mobile applications over a wireless connection. They may be connected to the internet directly over a wireless network, indirectly through an app, or sometimes not at all.

- **IP Cameras.** Cameras which, either wired or wirelessly, are connected to a local network. Being marketed to both businesses and consumers, their primary focus is for security and/or monitoring purposes. Most IP cameras offer the ability to view the camera feed using a web browser or mobile application and include automatic detection and alerting functionality.
- **Smart Locks.** Devices that add electronic locking/unlocking functionality to an existing lock, most often using a mobile application that communicates with the smart lock over a wireless signal. Typically the smart lock is either attached to an existing lock or replaces the lock entirely.
- **Baby Monitors.** The IoT baby monitor is essentially a camera and microphone that allows for parents to watch their small children through a mobile application. The device provides audio, video and in some cases also a speaker, allowing for some form of two-way communication to take place.
- **Smart Thermostats.** A thermostat that allows a consumer to control temperature remotely, often using both a mobile application and a separate physical device. These devices often gather statistics about temperature, usage behavior and energy consumption and can report this to the user.

The full list of IoT devices that have been tested can be found in “Annex A: IoT Device list” on page 65.

Through testing all these devices, we answer the following research questions, for each category separately as well as in general:

1. How secure is the software on popular consumer IoT devices?
    a. To what extent do the devices adhere to principles of *security* by design and by default?
    b. To what extent do the devices adhere to principles of *privacy* by design and by default?

More specifically, in this report the following aspects of security and privacy are assessed: secure access control, software updates, encryption, communication protocols, physical security and (un)authorized or unnecessary collection of consumer data.

From there, we answer the second research question:

2. What should be the minimum security requirements for IoT devices?

Where applicable we will give both category-specific and more general recommendations.

The rest of this report is structured as follows. Chapter 2 contains a detailed description of the methodology employed for evaluation of the devices. Chapters 3-8 cover the tested devices in detail, including specific findings and recommendations. Chapter 9 contains the score for each device, based on an evaluation of our testing scripts. A discussion of our findings and recommendations is found in Chapters 10 and 11 respectively.

2 METHODOLOGY

In this chapter we discuss the specific project scope and testing methodologies. In particular, this chapter provides details on the performed tests, the methods used in evaluating the specific devices as well as the scoring methodology used for the final evaluation. Also included is a description of the overall testing environment employed throughout the assessment. The methodology described here is not comprehensive, the devices are simply too different to capture all the tests we performed in such format. That said, if questions should arise, feel free to contact Strict for more specific details.

2.1 Scope

The scope of the tests is limited to the software running on the devices themselves. Explicitly out of scope are possible external resources that are used by the device, such as cloud resources. Physical security tests, such as communicating with the devices by attaching to onboard pinouts, are also out of scope, with the single exception of the smart lock category. For the smart locks category, physical security is of high importance, and is therefore analyzed as well.

2.2 Performed tests

Per device, several tests are performed following a test script. On a high level, the test script covers the following steps:

1. Unboxing of the device and installation of the device according to the manual (if present). During installation, capture all traffic.
2. Check if updates are available and install them. Capture all traffic that is generated.
3. Review the manual for privacy statements.
4. Analyze default device configuration.
5. Perform an automated Nessus scan of the device and manually verify any found results.
6. Perform a port scan of the device and test the exposed service for vulnerabilities.
7. Attempt to perform a Man-in-the-Middle attack on the communication.
8. Analyze the captured traffic, focusing on insecure communications and unnecessary transfer of data.

Based on these tests we interpret the results and see how the devices comply with security- and privacy principles. We focused on secure access control, software updates, encryption, communication protocols, physical security and (un)authorized or unnecessary collection of consumer data.

Since the scope is limited to the devices, possible internet resources that are used by the devices are not tested for vulnerabilities.

2.3 Overview of test environment

The test environment consists of a home-like local LAN environment where one of the acquired internet routers will operate the DHCP and DNS functionality. The LAN network will contain a wired networked Windows 10 PC and a wired network laptop with the testing software installed (see Figure 1 for a schematic overview).
Since most of the devices include a smartphone app, Android and iOS smartphones are also part of the test environment.

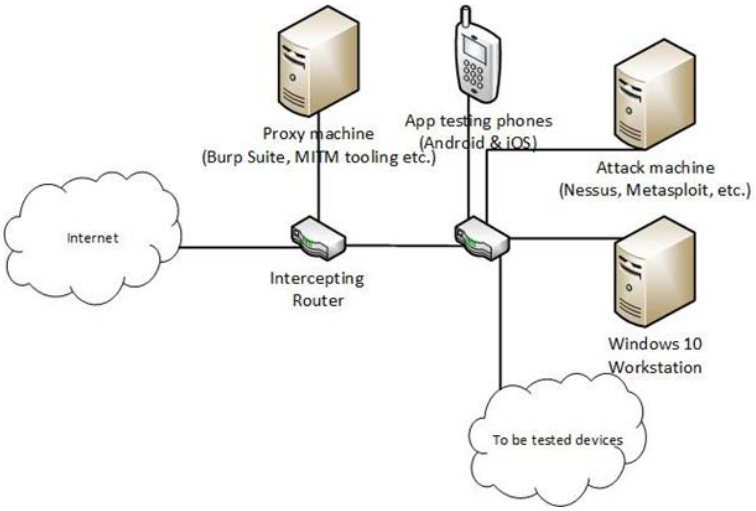

Figure 1: Schematic overview of test environment

2.4 Result scoring

For each device, the results are given a score with regards to the impact, probability and risk. Possible scores are 'negligible', 'low', 'medium', 'high' and 'critical'. The overall risk is calculated as risk = impact x probability, where impact indicates the severity of the consequences of exploiting the specific vulnerability and probability is the likelihood of an attacker exploiting the discovered vulnerability. For example, a low-probablity high-impact finding will generally result in a medium risk. Note that the scores are discrete labels but they represent a range of value judgements. Therefore, the reported risk value can sometimes be lower or higher than expected simply based of the score labels.

As mentioned before, part of the test process includes a Nessus vulnerability scan. As Nessus is an automated vulnerability scanner, we find it important to interpret the findings ourselves. This interpretation often led to a change in score. If a result is based on a Nessus finding, we report the risk score after our interpretation. The risk that was reported by Nessus will be included in parentheses.

2.5 Overall scoring

The overall scoring per device is inspired by OSSTMM. In OSSTMM, several aspects of the device are taken into account, and a score is given to each of these aspects. The scoring per aspect is measured against the maximum possible score, resulting in a total security percentage.

For the analysis in this research, a score is given for each of the aspects that is covered in the mentioned test script, with a total of 32 aspects. These aspects include for example which communication protocols are used, if automatic updates are possible and what kind of authentication is used for configuration changes. A weight is attached to each of the scores, depending on the importance for the overall security

of the device. Finally, the scores are compared to the maximum possible score, resulting in the overall security percentage.

Note that due to the way this percentage is constructed, it is mostly a measure of how many security issues exist and how severe they are. It is not necessarily an accurate estimation of actual security. If a device has a single critical vulnerability that fully compromises the device, the percentage score could still be relatively high if the device does everything else well. For that reason, we also include the most severe finding for each device.

Secondly, the scores per device should only be compared within their own categories and to a smaller extent compared to similar types of devices. For smart locks, for instance, the security considerations are different enough to make comparison with devices outside that category not very practical.

3 ROUTERS

This chapter provides an overview of the test results of the IoT devices in the category 'Routers'. Routers are devices which are used by consumers to connect to an Internet Service Provider and the internet.

Historically, routers are compromised through default passwords, lack of access control, lack of firmware upgrades, and hijacking of service-provider based provisioning protocols.

The impact of a hijacked router is severe. All traffic can be intercepted and it introduces severe risks for all internet-based transactions.

3.1 TP-LINK ARCHER C3150

3.1.1 Product description

The TP-Link Archer C3150 is a wireless router designed for household setups. The device has a 1.4GHz dual-core processor and four adjustable multidirectional antennas which result in good data performance during intended usage.

Figure 2: TP-LINK ARCHER C3150

The device comes with a concise quick-start guide and a clear manual which makes the configuration and installation of the device straightforward and easy.

A mobile application can be used to change the configuration of the router remotely. Registration with the manufacturer is not required. However, it is mandatory for remote administration via the app or to contribute to the online community.

3.1.2 Security

By default, the router has a standard set of security measures. The standard WiFi settings include WPA2-PSK by default. All connections to external cloud resources are initiated using TLS and are all within the EEA. DNS is used to resolve the addresses, which suggests that the device may be vulnerable to DNS attacks. The data transferred to the cloud has not been investigated, however we noticed that configuration changes pass through those cloud-based resources.

The device configuration can only be changed trough the web interface or through the mobile app, both of which require password authentication for changes. Although the initial connection with the web interface is performed over HTTP, the credentials are sent to the device encrypted with a public key that is retrieved from the device. Though this is a non-standard approach, this does prevent the credentials from being transmitted in plaintext and prevents the user from being presented an invalid certificate

error upon connecting. The default password is randomly generated. We could not find any patterns in the generation of these passwords, except for it using only numbers. During the initial configuration, the user is prompted to change the admin password. There are no password-strength requirements placed on this password. When configuring the wireless networks, the default password is filled in by default and is accepted as the new password. As this password is located on the device, this may compromise the network. Moreover, we do not consider 8-digit passwords adequately secure.

Software updates can be installed through the web interface and by using the app. Basic integrity checks on the used software are in place. It is possible to change the entire firmware, but this is not officially supported. Automatic updates are not supported. This provides a risk as critical vulnerabilities need to be patched as soon as possible. Relying on users to manually update could, especially without clear notifications, leave devices with unpatched software for long periods of time.

The manual describes how to share a plugged-in storage device (such as a USB stick) over the internet. This describes the steps to open an unencrypted FTP interface to the internet, which is a security risk.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
Medium	High	Medium	Initial wireless password configuration accepts default password, which is filled in by default.
Medium	Medium	High	Automatic updates are not supported.
Medium	Medium	High	Manual contains insecure instructions regarding FTP.
Low (Medium)	Negligible	High	(Nessus) SSH Server CBC Mode Ciphers Enabled Needs an existing SSH connection, which is very rarely utilized.
Low (Critical)	Negligible	High	(Nessus) Dropbear SSH, multiple vulnerabilities. CVE-2016-740{6,7,8,9}, CVE-2013-4434 The router uses a version of Dropbear SSH from 2012 for which multiple critical vulnerabilities are known. CVE-2016-7406 is applicable to remote attacks but requires control over the username or hostname. Since we lack said control this could not be exploited. The other vulnerabilities are exclusively client-side.
Low (Medium)	Low	Low	(Nessus) Web Application Potentially Vulnerable to Clickjacking. The attack surface is minimal due to sporadic usage of the web interface.

Low (Medium)	Negligible	Medium	(Nessus) SSH Weak MAC Algorithms Enabled. Needs an existing SSH connection, which is very rarely utilized.
Low (Low)	Negligible	High	(Nessus) Unencrypted Telnet server.
Low (Low)	Negligible	Medium	(Nessus) Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak).

Table 1: Findings for TP-LINK ARCHER C3150

3.1.3 Privacy

No specific Privacy Policy is included with the product, but a general Privacy Policy is published on the website for all products (not available in Dutch). The latest version is from June 15th, 2018. According to vendor information, updated versions will be published online. No specific notification will be sent to the users.

The Privacy Policy specifies in detail what personal data is processed and for what purposes. TP-link collects the basic personal information from users when using or registering the product, such as account details, payment details and IP addresses. Optionally, users can voluntary provide TP-link with extra information that potentially could be used to identify the user. This is extensively explained in the policy.

Users are clearly informed of their rights. The policy states that no personal data is being collected from children under the age of 13.

TP-link states they implemented measures, including encryption and SSL technology, designed to secure personal information from accidental loss and from unauthorized access, alteration, and disclosure. Indeed, insofar as personal information is transmitted from the device, that information is encrypted.

Overall this device complies with the minimal legal and regulatory requirements when it comes to privacy. Though not required, the device lacks a policy specific to the device. By default, unless the user enables remote administration, only very basic personal data, such as IP addresses, are collected.

3.2 Linksys MAX-STREAM EA7500

3.2.1 Product description

The Linksys EA7500 product is a mid-range wireless router, designed for household setups. The device operates on a version of Linux and a wireless app for remote control and configuration is available on iOS and Android. Remote control is disabled by default and must be manually enabled before it can be used. Features such as DMZ, firewall, port forwarding are available. Network Access Control is available on WiFi (WEP, WPA2) but not available on wired connections.

Figure 3: Linksys MAX-STREAM EA7500

3.2.2 Security

By default, the router has a standard set of security measures. The standard WiFi settings include WPA2-PSK by default. UPnP is by default enabled on this device which enables malware to open ports on the router. We observed connections connectivity to seven external resources outside of the EEA, including the download of firmware over HTTP. The most significant finding for these connections is the post of sensitive data to a cloud instance over HTTP, including base64-encoded admin credentials.

The remote control app requires the phone to be initially on the same network as the router. The admin page is accessible from the local network and allows plaintext/base64-encoded credentials which could be intercepted. Users are forced to change the admin password, but there are no minimum requirements for this password.

Firmware updates are possible from the internet but are triggered from the local administrator interface.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
Critical	Medium	Critical	The device posts sensitive data to a cloud resource, including base64-encoded admin credentials.
Medium (Critical)	Low	Critical	(Nessus) Portable SDK for UPnP Devices (libupnp) < 1.6.18 Multiple Stack-based Buffer Overflows (CVE-2012-5958 & CVE-2012-5959) The found vulnerabilities apply to UPnP version 1.3.1. The device applies an automatic update of the UPnP version after every reset for the default port 1900 to 1.6.1. A port scan found several other ports (49152-49154) still indicating UPnP version 1.3.1. When testing the range from 49152 to

			49154, none of the exploits succeeded as per the CVE description.
Medium	Medium	Medium	UPnP enabled by default
Medium	Low	High	HTTP Web configuration leaks credentials and other configuration information by default.
Medium (Medium)	Medium	Medium	(Nessus) SMB Signing not required
Medium (Medium)	Medium	Medium	(Nessus) Samba Badlock Vulnerability
Low (Medium)	Low	Low	(Nessus) Web Application Potentially Vulnerable to Clickjacking. The attack surface is minimal due to sporadic usage of the web interface.

Table 2: Findings for Linksys MAX-STREAM EA7500

3.2.3 Privacy

The Linksys EA7500 does not have a specific Privacy Policy, but on the website there is a general Privacy Policy available which applies to the website and all products and services offered by Linksys. A Dutch version of the Privacy Policy is available. The latest version is dated May 18, 2018. Updated versions will be published on website and they state users will be notified of any changes.

It is a very detailed Privacy Policy, which covers all products and services. When using this product, Linksys automatically collects certain personal data. This policy sums up in detail what personal data is being processed and for what purposes, but it is not clear which data they process regarding this specific router. They mention that they can receive personal data from third parties about their users, but it is not clear what kind of data they receive and for what purposes they receive it. Linksys will always ask for user permission before they approach users through direct marketing.

Users are clearly informed of their rights. The policy that that no personal data is being collected from children under the age of 13.

Linksys states that they strive to maintain appropriate administrative, technical and physical security measures designed to protect the information collected by the product. However, they mention that the transfer of information is never 100% secure.

Linksys appears to comply with the legal and regulatory requirements regarding the privacy policy. As we noted, the lack of a specific device policy creates uncertainty about what data is being processed regarding this device. However, if a router leaks credentials easily, which this one does, an attacker can subsequently monitor the entire network, which probably includes a lot of personal data. Therefore, in spite of the policy, using this device may pose a significant privacy risk.

3.3 ASUS RT-AC68U

3.3.1 Product description

Figure 4: ASUS RT-AC68U

The ASUS RT-AC68U Wireless-AC1900 router is high-end consumer router. It has 3 antennas and runs on Linux. Administration is done via the web interface or via an app. Remote control is disabled by default but can be enabled in the configuration. The device supports all the classic security controls for routers like DMZ, firewalling, port forwarding, filtering and logging.

3.3.2 Security

The basic web configuration server is HTTP and not encrypted, though this can be changed to HTTPS. Authentication credentials are sent in base64 and thus essentially plaintext. As such, an attacker sniffing the network can extract the credentials when the default HTTP option is used. The HTTPS option uses self-signed certificates and there is no evidence of certificate pinning. We observed connections to five resources outside the EEA, all of which are initiated using TLSv1.2.

Another salient point is that the device we tested runs on custom open source firmware, and not the official ASUS firmware. We could not necessarily find any flaws in this modified firmware, but it is not a conventional approach. Note that the base ASUSwrt firmware is partially open source as well.

Automatic updates are not supported. This provides a risk as critical vulnerabilities need to be patched as soon as possible. Relying on users to manually update could, especially without clear notifications, leave devices with unpatched software for long periods of time.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
Medium	Medium	High	Automatic updates are not supported.
Medium (Medium)	Low	High	(Nessus) Web Server Transmits Cleartext Credentials. In addition, configuration data including wireless credentials is also transmitted over the same connection in plaintext.
Low (Medium)	High	Low	(Nessus) DNS Server Cache Snooping Remote Information Disclosure
Low (Low)	Negligible	Medium	(Nessus) Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)
Low (Low)	Medium	Negligible	(Nessus) Web Server HTTP Header Internal IP Disclosure

Table 3: Findings for ASUS RT-AC68U

3.3.3 Privacy

There is no specific Privacy Policy, but a general Privacy Policy on the website for all Asus products (available in Dutch). The latest version is from May 23, 2018. Updated versions will be published on the website and they state users will be notified.

It is a very detailed Privacy Policy. When registering an account for using the Product, Asus collects basic user information, and users can optionally provide additional personal data, such as gender, address and profession for completing their account. Asus states they will never ask users to provide sensitive personal data and that they always ask for prior consent from the user when collecting personal data, for which the purpose is described in detail.

Customers are clearly informed of their rights. The policy states that no personal data is being collected from children under the age of majority as defined by the laws of the local country or region.

Asus mentions they take precautions to protect personal data against unauthorized access, alteration, disclosure or destruction. They conduct internal reviews of their data collection, storage and processing practices and technical and organizational security measures, as well as physical security measures to guard against unauthorized access to systems where they store personal data. Transmission of personal data between different locations of ASUS and its affiliated entities is performed through their secured wide area network. When users submit their personal data to Asus, the personal data is protected both online and offline. However, ASUS cannot guarantee perfect security on the internet.

Asus appears to comply with the legal and regulatory requirements regarding the privacy policy. As we noted, the lack of a specific device policy creates uncertainty about what data is being processed regarding this device. However, this device leaks credentials, allowing an attacker to monitor the entire network, which probably includes a lot of personal data. Therefore, in spite of the policy, using this device may pose a significant privacy risk.

3.4 Huawei B315s-22

Figure 5: Huawei B315s-22

3.4.1 Product description

The Huawei B315s-22 is a mid-range 4G router. It feels light and a bit fragile. It is possible to connect antennas, but these are not supplied. Surprisingly, there is an RJ11 port on the device. We were unable to determine the operating system of the router. It is possible to configure the device through a web interface and by

using a mobile app. A quick start guide is included, but a more detailed manual is not available. The quick start guide covers initial setup, but more advanced features are not described anywhere.

3.4.2 Security

Initial configuration is handled through a web interface or mobile app. For both options, a password is required. The connection is over HTTP, but the password is sent using a salted challenge response mechanism, which makes sniffing the password more difficult. Session information and cookies are sent over HTTP as well, thus the session can be hijacked. Remote management of the router is disabled by default but possible. During initial configuration, the user is forced to change the admin password and the default WiFi password. The usual WiFi security options are in place, and WPA2-PSK is enabled by default.

Automatic updates are enabled by default, and the check is done over HTTP, where versioning information is posted to an API. We were unable to downgrade the device to an earlier version, and internet research indicates that the update will be downloaded over HTTP. Although Huawei describes that a digital signature checking process is in place to mitigate this risk, we argue that updating over secure channels is a best practice that should be followed. We classify the potential impact of this as high, as the integrity of the update process can be compromised. The probability of this happening is considered to be low, resulting in a medium risk in our opinion.

We observed connections to two different external resources outside of the EEA, which are confirmed to be SNTP connections.

The web interface of the router exposes an API, in which we have found an unauthenticated information disclosure. This finding has been communicated to Huawei. The potential impact of the disclosed information is considered to be low.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
Medium	Low	High	HTTP Firmware update URL.
Low	Medium	Low	Unauthenticated information disclosure in web API
Low (Medium)	Low	Medium	(Nessus) SSL Certificate Cannot Be Trusted.
Low (Medium)	Low	Medium	(Nessus) SSL Self-Signed Certificate.
Low (Medium)	Low	Low	(Nessus) SSL Medium Strength Cipher Suites Supported (SWEET32).

Table 4: Findings for Huawei B315s-22

3.4.3 Privacy

There is no specific Privacy policy. There is a general Privacy policy on website for all Huawei products (available in Dutch). Latest version is from April 15, 2018. Updated versions will be published on website and users will not be sent a notification.

It is a very detailed Privacy Policy. Huawei is transparent about what personal data is being processed and for what purposes. Huawei collects certain basic personal information when using the product. When it comes to location data, users can choose the applications for which they want to enable location services. Huawei uses anonymous data to understand how users use their products and services and takes care that personal and anonymous data are strictly separated.

Users are clearly informed of their rights. Huawei will only process children's personal data if the parents have given their explicit permission. Huawei identifies whether those involved are children based on the age of majority defined by the laws of local countries and regions.

Huawei attaches great importance to the security of personal data and has adopted standard industry practices to protect personal data and prevent unauthorized persons from gaining access to the data, or making it public, using, changing, damaging or losing it. Huawei described extensively which measures they take. The two most important ones from the Privacy Policy are:

- We take reasonable and feasible measures to ensure that the personal data collected is minimal and relevant to what is necessary in connection with the purposes for which it is processed. We do not store your personal data for longer than necessary for the purposes stated in this Statement and Privacy Notice for a specific product or service, unless extension of the retention period is required or permitted by law.
- We use a range of technologies such as cryptographic technologies to ensure the confidentiality of data when transmitted. We implement trusted security mechanisms to protect data and data storage servers against attacks.

Overall this device complies with the minimal legal and regulatory requirements when it comes to privacy. Though not required, the device lacks a policy specific to the device, creating uncertainty about the particulars of this device. However, insofar as we can determine, communication to external servers that may contain personal data is encrypted. The amount of external resources that are accessed is considered a privacy risk. Completely taking over the device and subsequently monitoring the network seems more difficult for this device. Therefore, the privacy risk of utilizing this device is limited in that sense.

3.5 Netgear Nighthawk X4S R7800

Figure 6: Netgear Nighthawk X4S R7800

3.5.1 Product description

The Netgear Nighthawk X43 R7800 is a fairly high-end consumer router, sporting four antennas. Build quality is good, there is plenty of documentation available. The device responded well to extensive testing. Features include the standard set of router functionality, like DMZ, filtering options, port forwarding, etc.

3.5.2 Security

In terms of security, the Nighthawk R7800 is a mixed bag. We found only minor issues from our scans on an updated device. If the firmware is not updated however, several issues exist with respect to TLS and the underlying SOAP services. Since outdated versions are out of scope, we focus on the current version.

The current version of the R7800 communicates by default over a plaintext HTTP connection for both the web configuration and the local app configuration. It authenticates using HTTP Basic Authentication which means that all packets to the web server contain the credentials in base64-encoded plaintext. Therefore even a fully passive adversary can harvest credentials for the router. To make things worse, the WPA passphrases are also sent after initial login over that same HTTP connection in plaintext. If in local configuration mode, the Nighthawk app does the same thing.

The default HTTPS version uses a self-signed certificate and thus yields a certificate error in modern browsers. Things are a little better for the remote administration side of things. If the user enables remote administration via the Nighthawk app, that communication stream does use TLS for encryption. Connectivity with a single external resource outside of the EEA was observed, which is manufacturer-hosted. No significant amount of data was transferred.

The router has an option to support automatic updates, but this option has to be manually enabled.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
Medium	Low	High	Web Server Transmits Cleartext Credentials.
Low (Medium)	Low	Medium	(Nessus) SSL Certificate Cannot Be Trusted.
Low (Medium)	Low	Medium	(Nessus) SSL Self-Signed Certificate.
Low (Medium)	High	Low	(Nessus) DNS Server Cache Snooping Remote Information Disclosure.

Table 5: Findings for Netgear Nighthawk X4S R7800

3.5.3 Privacy

There is no specific Privacy Policy, but a general Privacy Policy on the website for all products (available in Dutch). The Latest version was published in April 18th, 2019. Updated versions will be published on website and users are notified of updates.

The published Privacy Policy is very detailed. Netgear indicates what personal data is processed and for what purposes. General personal information of users is requested and usage data such as IP addresses is collected automatically. Additional personal data, such as interests or hobbies, gender or age can also be collected by Netgear on a voluntary basis. Since this is not a product Privacy Policy, it is unclear which personal data is being collected specifically for this device.

Users are clearly informed of their rights. The policy states that no personal data is being collected from children under the age of majority as defined by the laws of the local country or region.

Netgear mentions that they take steps to remove or store personal information in a form that does not identify users when this information is no longer needed for the purposes for which they process it. They perform periodic evaluations of the databases and have set time constraints for the deletion of certain information, taking into account the type of service provided in the context of the products and services, the duration of our relationship with users, mandatory retention periods and the limitation period.

Netgear states maintains administrative, technical and physical security measures to protect personal information from accidental or unlawful destruction, accidental loss, unauthorized alteration, unauthorized disclosure or access, misuse and any other unlawful form of processing of personal information that they hold. They also contractually require that their suppliers protect such information against unauthorized access, use and disclosure

Netgear appears to comply with the legal and regulatory requirements regarding the privacy policy. As we noted, the lack of a specific device policy creates uncertainty about what data is being processed regarding this device. Similar to some of the other routers, however, this device leaks credentials. This allows an attacker to take control of the device and subsequently monitor the entire network, which probably includes a lot of personal data. Therefore, in spite of the policy, using this device may pose a privacy risk.

4 CONNECTED TOYS

Connected toys are attracting a lot of interest from the market as they provide new 'smart' capabilities to entertain both children and adults. As these toys are often aimed at children and young adults, privacy and security are critically important. Some of the toys do not connect to the internet directly, which reduces the attack surface significantly. However this does not excuse the lack of software updates and security fixes we have identified across most connected toys.

4.1 Vtech Storio Max Roze

4.1.1 Product description

The Vtech Storio Max is an Android tablet designed for children between the age of 3 and 11. The tablet is designed for educational purposes. The user can install multiple manufacturer-selected Android apps. The tablet has access to the internet and includes a built-in camera. Via a mobile application parents can communicate with children that are using the tablet via text, voice and images.

Figure 7: Vtech Storio Max Roze

4.1.2 Security

During the initial setup of the device, user accounts can be created. In order to do so, first a parent-user must be created. This user controls the configuration of the device (e.g. setting up WiFi and time limits for the child). The parent must set a simple 4-digit pin to protect the user. The child account can be set up afterwards, but this account cannot be protected in any way. This means that in case of theft or loss of the device, any messages or photos can be viewed by the person holding the device. As the device is aimed at children, who are prone to leave devices laying around, share toys or forget their device, this is considered a risk.

The parent is also asked to create a cloud account, which can be used for communication between the parent using the app and the child using the tablet. This account is protected using a combination of username and password. The password requirements are relatively secure. There is no option for two-factor authentication.

The device itself does not broadcast a WiFi signal, but can be connected to WiFi. Communication streams, both of the app and the device itself, appear to be safe and secured against Man-in-the-Middle attacks. While scanning the device no vulnerabilities were found and no ports appeared to be open. We observed connections with five resources outside of the EEA, all of which use TLSv1.2. No significant amount of data was transferred.

Automatic updates are not supported for this device.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
High	Medium	Critical	Unauthenticated access to child account on device. As children are not very careful with their devices, this provides a high risk.
Medium	Medium	High	Automatic updates are not supported.

Table 6: Findings for Vtech Storio Max Roze – Kindertablet

4.1.3 Privacy

There is no specific Privacy Police available, but a general Privacy Policy on the website for all Vtech products (available in Dutch). The latest version is from September 11, 2018. Updated versions will be published on the website and users will be sent a notification.

Vtech states that they will inform users about what personal data is processed and for what purposes. General personal data of users is required for using the product. Sensitive data will not be processed, unless users provide it to Vtech on their own initiative. Vtech states that while using this product, certain personal data, including but not limited to text messages, voice messages, or photos, may be sent by your child to specific recipients. This is not possible without this data being processed and stored via the VTech service.

Users are clearly informed of their rights and retention periods are mentioned in the Privacy Policy. This product is primarily designed for the use by children. However, VTech will not process children's personal data without prior approval from parents.

VTech states they take appropriate technical and administrative security measures to protect personal data against intentional or accidental manipulation, partial or complete loss, destruction or unauthorized access by third parties. In addition, their security measures are supposedly continuously improved as a result of technological developments.

More specifically they mention:

- We use measures to protect your data against accidental loss or unauthorized access, use, destruction or disclosure
- We limit access to personal data
- We implement appropriate (control) measures, including supervision and physical measures, for safe storage and transfer of data
- We periodically perform data protection impact assessments in accordance with legal requirements and our company policy.

Overall, Vtech complies with the legal and regulatory requirements regarding privacy. That said, there are definite privacy risks involved with the unauthenticated child account. Whilst Vtech may have limited access to that data, anyone with physical access to the device can view al the information a child may have stored, including pictures and other media.

4.2 Spider-Man Interactive App-Enabled Superhero

4.2.1 Product description

The Spider-Man interactive app-enabled superhero is a connected toy that allows several forms of interaction. As the name suggests, an app is needed to make full use of the toy. It is clear that significant attention has been put into the design and production of the toy, it feels robust and has lots of details.

Depending on the feature used on the toy, voice response is triggered. We found this to be somewhat unreliable. The toy only communicates in English.

Figure 8: Spider-Man Interactive App-Enabled Superhero

4.2.2 Security

Initial configuration of the toy is done via Bluetooth, during which a WiFi connection is established. The toy is able to function on just Bluetooth, but as long as WiFi with an internet connection is available, communication between app and toy is done via the cloud. These connections are established using TLS.

During the initial configuration a check for updates is performed as soon as an internet connection is available. Since no updates were performed, we could not verify if the integrity of the update is verified. Software updates can be triggered, however there is no feature to manually install updates. Scanning of the device revealed no open ports. The Nessus scans returned only some informative results.

A successful Man-in-the-Middle attack was performed on the mobile app by using Burp Suite. The app does verify the certificate that is presented, but if it can be verified up to a trusted root present in the truststore on the smartphone, the connection is established. The app communicates with the toy via a cloud-based API. During the Man-in-the-Middle attack, the credentials that are used to post requests to the API were found. To communicate with the toy, a device ID and a token are required, which were also found in the requests. We were able to replay requests to which the toy responded as if these requests were sent from the app.

Since the API is cloud-based, we did not perform any additional attempt to see if we could compromise other Spider-Man accounts through the API.

We also attempted a Man-in-the-Middle attack on the toy itself, by rerouting all the traffic through Burp Suite. The toy did perform some connectivity checks through our proxy at startup, but did not accept our rogue certificate for the cloud resources it connected to. Since we had no access to the toy's OS, we

could not install our CA in the trust-store, making it impossible to intercept the traffic between the toy and the cloud resources. In total fifteen different external IP addresses outside of the EEA were accessed, all of these connections use TLSv1.2. Large amounts of data were transferred.

The device automatically installed firmware and software updates.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
Low	Negligible	High	No certificate pinning in the mobile app.

Table 7: Findings for Spider-Man Interactive App-Enabled

4.2.3 Privacy

There is a specific product Privacy Policy on the website (not available in Dutch). The latest version is from May 20th, 2018. Updated versions will be published on the website and users will not be sent a notification.

Sphero has published a very detailed Privacy Policy that is specific to this product. For toy configuration, the age of the user will be requested. If children are under 13 (or under a specific age as local law dictates), providing their email address is optional. When using his device, Sphero can collect sensor data from the microphone, camera or location data of the device to let children interact with the device or to enable Guard mode. Sphere will always obtain consent in the application before collecting such data.

Users are clearly informed of their rights. The Privacy Policy does not specifically mention information about security. However, the Sphero website contains a lot of information regarding both data storage, privacy and the measures taken in that regard.

Overall, Sphero complies with legal and regulatory requirements in their Privacy Policy. The device sends a lot of possibly sensitive information to the cloud, in particular microphone sensor data. However, if the information they publish is accurate, great care is taken with respect to securing this data. We did not find anything that disproves Sphero's claims.

4.3 MAKEBLOCK Codeybot Wit

Figure 9: MAKEBLOCK Codeybot Wit

4.3.1 Product description

The Codeybot is a well-built and sturdy device, aimed at teaching children how to program computer code. The device consists of two wheels and a screen with a limited number of LEDs that represent pixels and can be used to display messages or 'faces'. The device uses an application called 'Codeybot' that is used to control the device.

The manufacturer has removed several pages that referred to this product. This results in the included documentation and manual being outdated, as mentioned URLs do not exist anymore. Newer versions on the manual or firmware updates could also not be found on the manufacturers website.

4.3.2 Security

As the device is not directly connected to the internet and no indirect internet connection is made through the mobile application, the risk for hijacking from the internet is considered low. Setting up the device is done by connecting to the device's access point, which it broadcasts by default, and opening the Codeybot app. This access point does not have a password, which allows anyone to connect to the device. After connecting to the access point, it is possible to SSH to the broadcast IP as root and log in without password, thereby gaining full access to the device's functions and control the device.

As the device does not have any sensors like cameras or microphones, the device cannot be directly used to gather personal information by an attacker, especially since the device is on a separate network. However, it is possible to send audio files (including voice recordings of a potential attacker) to the device and play these.

The product does not seem to have an easy way to update the firmware, nor supports automatic updates, which prevents any security risks to be mitigated.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
Critical	High	Critical	Unauthenticated root access to device.
High	Medium	High	Not possible to update device.
Low (Critical)	Negligible	High	(Nessus) Dropbear SSH, multiple vulnerabilities. CVE-2016-740{6,7,8,9}, CVE-2013-4434 The device uses a version of Dropbear SSH prior to 2016 for which multiple critical vulnerabilities are known. CVE-2016-

			7406 is applicable to remote attacks but requires control over the username or hostname. Since we gained root access through other means, we did not further investigate this vulnerability.
Low (Medium)	Low	Low	(Nessus) Web Server Generic XSS.
Low (Medium)	Low	Low	(Nessus) Web Application Potentially Vulnerable to Clickjacking.
Negligible (Medium)	Negligible	Low	(Nessus) IP Forwarding enabled.

Table 8: Findings for MAKEBLOCK Codeybot Wit

4.3.3 Privacy

There is no specific product Privacy Policy, but a general Privacy policy on the website which applies to the use of the website and all products and services offered by Makeblock (not available in Dutch). The latest version is from March 29th, 2018. Updated versions will be published on the website and users will be notified of any changes.

The Privacy Policy is very detailed and states that Makeblock will inform users about what personal data is processed and for which purposes. Explicit and informed consent will always be asked before sharing personal data or using data for a purpose other than mentioned in the Privacy Policy. In the Privacy Policy is mentioned that personal data is being asked that can be used to identify and/or contact a natural person. This includes name, postal address, organization etc. That also includes job description and scope of business operations. It is unclear for what purpose they use some of this information. In addition, it is not clear what specific personal data is being processed by using the Codeybot.

Makeblock processes personal data not only on servers in the EU, but also in the US, China or Japan. It is also mentioned that personal data will be kept until a customer deletes his/her account. Nothing is mentioned whether the data is deleted under other circumstances without specifically being prompted by the user. This makes it unclear whether Makeblock complies with EU law in terms data retention.

Users are clearly informed of their rights. There is nothing mentioned about children's personal data.

Makeblock states they use a variety of security measures to maintain safety of personal data. They encrypt many of their services using TLS when transmitting data. Hashing is used when storing passwords. They review information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems.
We cannot say for certain Makeblock complies with EU laws and regulations as it is unclear for which purposes certain data is collected. Additionally, as we mentioned, there are some possible issues regarding data retention.

The device is insecure, but it is unlikely that this introduces significant privacy risks as no personally identifiable information is stored on or available to the device.

4.4 RC Spy Tank with Camera

Figure 10: RC Spy Tank with Camera

4.4.1 Product description

The RC Spy tank is an app-controlled tank with a camera. In terms of functionality it is a fairly limited device, it can only be controlled with a smartphone app and offers a video feed. The app allows to make recordings and pictures of the video feed.
It was unclear which app was to be used with the device. Several apps that suggest that they are made for this tank are not able to connect to the toy. Furthermore, the WiFi connection to the toy is very unreliable. Establishing a connection often fails, requiring a reboot of the device. Once a connection is established, it does seem to be persistent.

4.4.2 Security

There is no security enabled on the device. As the device is not directly connected to the internet and no indirect internet connection is made through the mobile application, the risk for hijacking from the internet is considered low. Connecting to the tank does not require any authentication. The toy creates a WiFi access point, to which a phone must be connected for the app to work. It seems that the number of connected devices is limited to one, as we were unable to connect multiple phones or devices to the toy. This could also be a consequence of the very unreliable WiFi connectivity as well. Since no authentication is required, anyone can connect to the toy when in range and view the video feed if the correct app is used. The WiFi connection does not use any encryption, so the video feed can also be viewed by sniffing the WiFi signal.

Port scans revealed a web interface through which the access point settings can be managed. Authentication is required but uses predictable credentials. Two other open TCP ports exist, one for the video feed (8080), which can be accessed using an RTSP client, and the other port is used to control the tank (8081). We did not spend any time on reverse engineering the commands that are sent to the tank, since one can simply install the app and use that.

No reference to the (automatic) installation of firmware updates was found, meaning that vulnerabilities present in the device cannot be remedied.

The following table summarizes our findings.

Risk (Nessus)	Probability	Impact	Description
Critical	High	Critical	Unauthenticated access to device. Since the device has a camera, the impact is considered to be critical.
High	High	High	Predictable credentials on the web interface.
High	High	High	Unauthenticated RTSP stream.
High	High	High	Unencrypted access point by default.
High	Medium	High	Not possible to update device.

Table 9: Findings for RC Spy Tank with Camera (ATTOP)

4.4.3 Privacy

For this device no privacy statements were found. Considering the lack of encryption on the communication from the device and the availability of a video feed the toy does not comply with any privacy by design best practices. Anyone within wireless range can simply eavesdrop on the video stream. As such, we conclude that this device is a definite privacy risk.

4.5 I-Spy Tank with Camera

Figure 11: I-Spy Tank with Camera

4.5.1 Product description

The i-Spy tank is an app-controlled tank with a camera. In terms of functionality it is a fairly limited device, it can only be controlled with a smartphone app and offers a video feed. The app allows to make recordings and pictures of the video feed.

When driving the tank around, the video feed is updated relatively slowly, which makes it hard to drive. The tank feels quite robust and looks decent. The app and manual are very basic and are written in very poor English.

4.5.2 Security

Security measures on this toy are nonexistent. The toy creates a WiFi access point to which a phone must be connected for the app to work. Since this is an access point and not an ad hoc WiFi network connection, anyone can connect to the device while it is powered-on. Another person that has installed the app on his/her phone can connect to the device and view its video feed. There is no password protection in place. When using the default settings, there is no encryption in place for the WiFi connection. This allows an eavesdropper to view the video feed by simply sniffing the WiFi signal.

Port scans revealed a web interface, through which the access point settings can be configured. This interface requires a username/password, for which the default password can be found on the internet easily. There is also an anonymous FTP service, through which the entire file system is accessible. This includes write privileges, but the device uses a volatile storage system since after a reboot any stored files are no longer present. A port offering a video feed was also found, to which one can simply connect a video player which supports the type of stream. Another open port that was found exposes an interface that controls the tank movements. Sending simple commands to this interface allows an attacker to control the device without using the app. There are two ports that allow SMB clients to connect, but there are no accessible shares. The last open port that was found contains a UPnP service, which is likely an artifact of the access point software the device is built on.

No reference to the (automatic) installation of firmware updates was found. Therefore, any vulnerabilities or other issues cannot be remedied at a later date. Further, the official app does not support iOS version 10 or above, which means that an iPhone that wants to run the app is not up to date and therefore more vulnerable. As the device is not directly connected to the internet and no indirect internet connection is made through the mobile application, the risk for hijacking from the internet is considered low.

The following table summarizes our findings.

Risk (Nessus)	Probability	Impact	Description
Critical	High	Critical	Unauthenticated access to device. Since the device has a camera, the impact is considered to be critical.
High	High	High	Predictable credentials on the web interface.
High	High	High	Unauthenticated RTSP stream.
High	High	High	Unencrypted access point by default.
High	Medium	High	Not possible to update device.
Medium	High	Medium	Anonymous ftp service with root read privileges and write privileges in some directories.

Table 10: Findings for United Entertainment – I-Spy Tank with Camera

4.5.3 Privacy

For this device no privacy statements were found. Considering the lack of encryption on the communication from the device and the availability of a video feed the toy does not comply with any privacy by design best practices. Anyone within wireless range can simply eavesdrop on the video stream. As such, we conclude that this device is a definite privacy risk.

5 IP CAMERAS

IP cameras are one of the most used IoT devices on the consumer and business market. They are heavily discussed devices when it comes down to both security and privacy aspects. IP cameras are available in different shapes and sizes. Functionality ranges from a basic set to an extensive number of different functions. As these devices have access to live imaging and audio in a consumer environment, GDPR legislation concerning children can classify the data as more sensitive. For this reason, we expect utmost care around IP camera devices from the manufacturers.

5.1 Ubiquiti UniFi Video Camera G3

5.1.1 Product description

The Ubiquiti UniFi G3 is a network-enabled video camera that can be used within a UniFi video surveillance management system. The camera can record 1080p HD video and is suitable for both indoor and outdoor use. The device uses PoE and can be used on the local network via an app or a web interface.

Figure 12: Ubiquiti UniFi Video Camera G3

We found the app to be unreliable. The device would appear as being disconnected, while the connection was up and stable via the web interface.

5.1.2 Security

As the device works solely over an ethernet cable, security risks that would often apply regarding the use of WiFi do not apply for this device. Other than during the registration in the mobile application, no data transmission to external servers was found. Data that was sent to external servers during the registration, as well as data sent over the local network, uses a TLSv1.2 connection following industry standards. We observed connections with three unique IP addresses outside of the EEA. No significant amount of data was transferred.

Upon installing the device, we found that the device uses the same username and passwords for all devices. During configuration we were not forced to change this password. The device does not automatically update unless it is connected to hardware that manages the UniFi video cameras, such as the UniFi Network Video Recorder.

The Nessus scan did not yield any vulnerabilities. Some informative findings were reported, such as the ability to guess the device type, detect the card manufacturer, the MAC address and several open ports. None of the open ports were running services that are exploitable.

By itself, the device does not support automatic updates. Firmware updates can be manually installed via the web interface.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
Medium	Medium	High	Default credentials are used which are not forcibly changed during config.
Medium	Medium	High	The stand-alone device does not support automatic updates.

Table 11: Findings for Ubiquiti UniFi Video Camera G3

5.1.3 Privacy

There is no specific Privacy Policy, but a general Privacy Policy on the website for all Ubiquiti products (not available in Dutch). The latest version is from June 15, 2018. Updated versions will be published on the website, but no notification will be sent to users.

The detailed Privacy Policy states that Ubiquiti will inform the user what personal data is processed and for what purposes. They collect user provided information, such as name, mailing address and other contact information. They also collect usage data, but they specifically mention that they do not collect the content of any communications that passes through their devices. They share data with third-parties for marketing, research or similar purposes, but they always use aggregated or deidentified information.

Data is stored in the US, but Ubiquiti complies with the EU-US Privacy Shield Framework.
Users are clearly informed of their rights. No personal data is being collected from children under the age of 13.

Ubiquiti describes that they believe that they have implemented commercially reasonable precautions to protect the user information from loss, misuse, and unauthorized access, disclosure, alteration and destruction.

Overall, Ubiquiti complies with legal and regulatory requirements with respect to their policy. As the policy is not specific to the device it is uncertain what data is collected by this device in particular.
Additionally, if default credentials are used an attacker can get easy access to the device, allowing monitoring of the video stream. That may expose sensitive information and thus is a privacy risk.

5.2 Hikvision DS-2CD2385FWD-I

5.2.1 *Product description*

This Hikvision IP camera is a network-enabled security camera intended for both home and business use. It can be configured for use in many types of network environments as long as it can be connected over ethernet, since it requires PoE. Configuration options include recording schedules, external data storage, motion detection and other event recognition.

Figure 13: Hikvision DS-2CD2385FWD-I

5.2.2 *Security*

The security of the device, if the user updates the firmware, is quite good. There are a number of known issues with Hikvision cameras for older firmware versions but none of them apply after firmware updates are in place. The default settings do not appear to leave the user vulnerable to attacks. The issues found relate to the TLS setup. The web configuration allows TLSv1.1 and uses self-signed weakly-parameterized certificates, which does not comply with industry best practices. The same web configuration is reachable through plain HTTP and the manufacturer uses some encryption on the data there as well. While unconventional, we were not able to break the scheme within a reasonable amount of time.

The Hik-Connect app can be used in authenticated mode and guest mode. It communicates securely, using well-configured TLS connections to API servers. That said, the guest/visitor mode shows cached devices from the authenticated mode. It allows configuration changes to be made in that mode. An attacker with access to the app but not to the camera credentials can therefore view the stream and make certain configuration changes (e.g., change the time and date).

Updates need to be installed manually, as automatic updates are not supported. Although we understand the consideration of camera-feed availability versus the security of automatic updates, the risk still applies

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
Medium	Medium	High	Automatic updates are not supported.
Medium	Low	Medium	Access to camera while using app in guest mode.
Low (Medium)	Low	Medium	(Nessus) SSL Certificate Cannot Be Trusted.
Low (Medium)	Low	Medium	(Nessus) SSL Self-Signed Certificate.
Low (Low)	Negligible	Low	(Nessus) SSL Certificate Chain Contains RSA Keys Less Than 2048 bits.

Table 12: Findings for Hikvision DS-2CD2385FWD-I

5.2.3 Privacy

The Privacy Policy is available when installing the camera and available online. This is a not a specific product Privacy Policy, but a general Privacy Policy which applies to the services for using products from Hangzhou Hikvision Digital Technology Co. This includes using the websites (user account) or the software which can be downloaded for applications on mobile devices. (Not available in Dutch). The latest version was published March 14th, 2019. Updated versions will be disseminated through e-mail specified in a user account or by means of notice on the website or app.

The Privacy Policy is clear and Hikvision is transparent about what information they collect and for what purposes. Prior express consent is needed for marketing purposes and users have the right to opt out of the use of their personal information for this marketing purpose. Personal information is being anonymized when shared publicly or with third-parties for marketing or analytics.

Users are informed of their rights. No personal data will be collected by children under the age of 18, or equivalent minimum age in the relevant jurisdiction.

Hikvision states they have implemented commercially reasonable administrative, technical, and physical security controls that are designed to safeguard personal information. They also conduct periodic reviews and assessments of the effectiveness of their security controls.

Apart from this Privacy Policy, in the user manual they mention they do not take any responsibility for privacy leakage or other damages resulting from cyberattack, hacker attack, virus inspection or other internet security risks.

Overall, Hikvision complies with legal and regulatory requirements with respect to their policy. As the policy is not specific to the device it is uncertain what data is collected by this device in particular. Communications security on this particular device does not conform with industry best practice across the board, which introduces some privacy risks.

5.3 Foscam C1

Figure 14: Foscam C1

5.3.1 Product description

The Foscam C1 is a network-enabled security camera intended for home use. The camera can detect human presence by using heat signatures and sends alerts for motion and sound changes. It uses passive infrared detection to sift through moving objects to avoid false positives.

The device can be used in combination with a mobile application for managing alerts and configuration as well as viewing live video feed. The device has an SD-card slot so files can be stored locally.

5.3.2 Security

During the initial configuration, a soft access point is used for setup. That same WiFi is used for connecting to an existing wireless network after configuration is complete. It is possible to configure the device using the web interface, however the app provides the user with more functionality and remote access. The web configuration is odd in that HTTPS is an option theoretically, but only HTTP is supported on the login page. We observed connections to nine resources outside of the EEA, consisting of cloud resources and vendor hosted domains.

The default password is blank and the user needs to create a new password at first login. Further, it has basic user administration controls and a fairly limited “firewall” capability.

There are a number of known issues with Foscam cameras for older firmware versions but none of them apply after firmware updates are in place. Users are definitely advised to update as soon as possible. The device does not automatically update the firmware. Although we understand the consideration of camera-feed availability versus the security of automatic updates, the risk still applies (but is accepted). The update process is improved when compared to older versions of the camera, since only a single firmware file needs to be uploaded instead of two.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
High	Medium	High	Login only possible over HTTP.
Medium	Medium	High	Automatic updates are not supported.
Medium	Low	High	Firmware updates over HTTP.
Low (Medium)	Low	Medium	(Nessus) SSL Certificate Cannot Be Trusted.

Low (Medium)	Low	Low	(Nessus) Web Application Potentially Vulnerable to Clickjacking.

Table 13: Findings for Foscam C1

5.3.3 Privacy

There is no specific product Privacy Policy available, but a Privacy Notice for all products on the website (not available in Dutch). Updates will be published on the website. The latest version is from April 12, 2018.

The Privacy Policy states that Foscam will inform the user what information is collected and for what purposes. The Privacy Policy is not a product specific. The data collection policy is for this product is undefined. Foscam publishes detailed information about their data collection and retention policies. It is striking that Foscam emphasizes that national legislation may impose certain requirements when using camera surveillance and that the user must pay close attention to this.

Users are informed of their rights. No personal data will be collected by children under the age of 18, or equivalent minimum age in the relevant jurisdiction. Parents' written consent should be obtained prior to the use of Foscam products.

Foscam mentions they strive to secure user information to prevent leakage, improper use, unauthorized access or disclosure. They will use a variety of measures to ensure the security of information within reasonable security standards. For example, they will use encryption technology and other means to protect personal information.

They indicate that they have set up specialized management systems, processes and organizations to ensure the security of information. For example, they strictly limit the range of people who may access such information and require them to comply with the confidentiality obligations.

Overall, Foscam complies with legal and regulatory requirements with respect to their policy. As the policy is not specific to the device it is uncertain what data is collected by this device in particular. Communications security on this particular device does not conform with industry best practice across the board, which introduces some privacy risks. The amount of resources outside of the EEA that are accessed by the device is also considered a privacy risk.

6 SMART LOCKS

The smart lock category is relatively new in the Dutch market, it is growing fast, and the security of devices is very important as it is linked to physical security. In the consumer market this can have a direct impact on personal security at home. For this reason, we have high expectations for management of vulnerabilities, software updates and also specifically the vulnerability to physical attacks.

The main attacks we investigated for smart locks besides general vulnerabilities are replay-attacks, relay-attacks and physical attacks.

Normal (old-fashioned) locks are also sensitive to physical attacks, but we noticed that with smart-locks a simple button press can be enough to unlock, where this requires the turning of a lock, or handgrip in mechanic locks.

Replay attacks will record the WiFi or Bluetooth session and try to replay this to open the lock.

Relay attacks will put a relay between the 'key' application and the lock to present the lock with an idea that the 'key' application is nearby. Relay attacks are very common in smart locks found in for example automobiles.

6.1 Nuki Smart Lock

6.1.1 Product description

The Nuki Smart lock is an electronic locking device primarily for home use. The device is installed on the inside of the door and provides locking and unlocking via Bluetooth, through either the app or (optionally) automatically when the user is in close proximity. In addition, the device can be operated manually. The device works by manually inserting a key and mounting the lock on top of the existing cylinder.

Figure 15: Nuki Smart Lock

6.1.2 Security

Nuki has performed an external audit of the device's system security by Zillner IT-Security. They found no critical problems with the device. Indeed, we also found no problems with the technical implementation of the device. The app communicates securely with external uses over a TLSv1.2 connection. Certificate pinning is in place, and thus performing a Man-in-the-Middle attack on the TLS connection becomes infeasible. They have implemented an unspecified encrypted protocol on top of Bluetooth LE. The protocol is resistant against information disclosure and replay attacks. This is evidenced by the use of non-deterministic encryption. We were able to Man-in-the-Middle the

Bluetooth connection ourselves. Indeed, the device was resistant to replay attacks but relay attacks are still a risk, especially when automatic locking/unlocking is enabled.

The default settings of the device could be more secure. By default the button on the device allows for locking/unlocking. The button also allows Bluetooth pairing with a new device when held down for 5+ seconds. This is a potential physical security problem if an attacker can access the button on the device through other means. In particular, inserting a tool that presses the button through, for instance the letterbox opening, subverts all the security controls in place completely by either unlocking the door or pairing with the attacker's mobile device. There are good arguments for allowing unlocking from the inside (the ability to escape in case of emergency, primarily) without keys, but we feel the button press option is unnecessary since the device also provides a rotating lock/unlock function.

Software updates are supported via the mobile application and must be manually triggered. Seeing as the device is not directly connected to the internet and the risk of automatically updating the lock may be larger than having no automatic updates, we did not classify this as a risk. For example, automatic updates may fail or brick the lock without the users being aware.

The following table summarizes our findings.

Risk (Nessus)	Probability	Impact	Description
High	Medium	Critical	Insecure default settings regarding physical security.
Medium	Low	Critical	Potential relay attack.

Table 14: Findings for Nuki Smart Lock

6.1.3 Privacy

There is no specific product Privacy policy available, but Nuki has published a general Data Protection Declaration on their website for all Nuki products (not available in Dutch). The latest version was published in May 2018.

The Policy is not very detailed and does not specifically focus on the smart lock. Nuki processes personal data that they receive in the course of their business relation with the user. Personal data is being collected from the user or third-parties, such as partner companies. It is not known which third-parties.

When using the Nuki app and webservices for the use of the door Lock, Nuki describes the personal data they collect and process in the course of registering and then using Nuki. In addition, they collect personal data such as age, sex, language, interests and country of residence. They describe that this data is collected in the course of registering and using a Nuki-developed app for using the lock. It is not defined why they require this specific data.

Customers are informed of their rights. Nothing is mentioned in this Privacy Policy about the personal data of children.

In the Privacy Policy nothing is described about security.

As we noted above, there are some undefined behaviors and/or processes in the policy. However, the device does not appear to store or transmit personal data. None of the security issues directly lead to privacy risks.

6.2 Danalock V3

6.2.1 Product Description

The Danalock V3 is a smart locking device for home use. Like all the other smart locks, it is installed on the inside of the door and uses Bluetooth for (un)locking a given door with a mobile application. Features include automatic (un)locking based on proximity, "Twist-Assist" for easy manual (un)locking, logging and monitoring. Registration with Danalock is necessary in order to add locks to the app.

Figure 16: Danalock V3

6.2.2 Security

Our research indicated that previous versions of the Danalock contained vulnerabilities. After testing we found that none of these apply to the current version of Danalock. In addition, we were not able to find other technical vulnerabilities. We attempted to Man-in-the-Middle the communication between smartphone and lock, but were not successful. The Danalock does not reply to requests sent as Man-in-the-Middle. As such, we could not mount the classic relay or replay attacks.

No secondary authentication mechanism is available on the device, e.g., a PIN. This means that an attacker that gains access to the phone also gains access to the cached locks.

In terms of physical security, it is feasible that if an attacker can insert some small tool through a letterbox opening or another small gap, the attacker could then open the door by handling the manual locking/unlocking functionality. In this case, the attacker would need to grip and turn the handle on the device. With twist-assist enabled, this is made easier to do as the handle only needs to be turned a few degrees.

Software updates are supported via the mobile application and must be manually triggered. Seeing as the device is not directly connected to the internet and the risk of automatically updating the lock may be larger than having no automatic updates, we did not classify this as a risk. For example, automatic updates may fail or brick the lock without the users being aware.

The following table contains a summary of our findings.

Risk (Nessus)	Probability	Impact	Description
High	Medium	Critical	Physical security design issue.
Medium	Low	Critical	No secondary authentication option available when starting the app.

Table 15: Findings for Danalock V3

6.2.3 Privacy

There is no specific product Privacy Policy. On the website a general Privacy Policy for all Danalock products (not available in Dutch) can be found. The latest version is dated May 25, 2018. New versions will be published on the website. No notification will be sent to users.

The Privacy Policy states that the Danalock application receives user information entered by users when they register. This Policy states that Danalock makes an effort to collect only the personal data that is necessary for using the device and/or legal or contractual compliance. The processing is necessary to pursue their legitimate interest regarding the administration of their business and meeting their obligations to customers. In addition, the application can automatically collect certain data, including but not limited to, the type of mobile device you use, your mobile device's unique entity ID, the mobile device's IP address, your mobile operative system, the type of mobile internet browsers you use and information about how you use the program.

In the Privacy Policy it is stated that personal data is primarily collected from the data subjects. Danalock also collect certain information from other sources, including public databases. The other sources are not specified.

Users are informed of their rights. Danalock does not use the application to request personal data from children.

Danalock states that they ensure the confidentiality, integrity and accessibility of the personal data processed by them through the implementation of technical and organizational security measures.

Overall, the Privacy Policy complies with legal and regulatory requirements. However, there are some uncertainties with respect to which data is actually processed. Additionally, mandatory registration of a Danalock account is not necessary for the core functionality of the device. The access logs are stored online and not (only) on the device itself. This does not comply with principles of data minimization.

6.3 Nemef Entr

Figure 17: Nemef Entr

6.3.1 Product Description

The Nemef Entr is a smart lock for home and business use. The user can (un)lock the device using a smartphone as well as other (purchasable) options like fingerprint scanners and keypads. The device is affixed to the cylinder, or alternatively the provided cylinder can be used for easy installation.

6.3.2 Security

The Nemef Entr communicates solely over a Bluetooth LE connection. We were able to Man-in-the-Middle the connection with some success, but this did not lead to any replay attacks. Relaying the communication proved unreliable but possible to some extent, meaning that these kinds of attacks are still a possibility. The device does not seem to communicate to outside servers for its functionality. A disabled firmware version checking mechanism is in place that might communicate with external servers if it were enabled.

There is the option to secure the app with a PIN as well, which helps in the event an unauthorized user gains access to the mobile device. This feature is not turned on by default.

In terms of physical security, the Nemef Entr is considered sufficient. When the device is mounted on a secure door, it will provide sufficient security and convenience. Physical access to the device through a letterbox can breach security. The press-and-turn function provides a more secure option than single button unlock feature found in other smart locks.

Software updates are supported via the mobile application and must be manually triggered. Seeing as the device is not directly connected to the internet and the risk of automatically updating the lock may be larger than having no automatic updates, we did not classify this as a risk. For example, automatic updates may fail or brick the lock without the users being aware.

The following tables summarizes our findings.

Risk (Nessus)	Probability	Impact	Description
Medium	Low	Critical	Physical security design issue.

Table 16: Findings for Nemef Entr

6.3.3 Privacy

On the website there is a general Privacy Policy for all Nemef services. The date is not specified and updates will be published without notification to users. Nothing is mentioned about privacy specifically

for the use of this product. That said, the Nemef Entr does not use or require internet services. The smartphone and the lock are only connected by Bluetooth.

In general however, users of Nemef products are informed of their rights.

Nemef mentions they place great importance on user's privacy and ensure that personal data is treated confidentially and with the greatest possible care. They have therefore taken appropriate technical and organizational security measures against loss, theft or otherwise unlawful processing of this data.

While Nemef has published a Privacy Policy, it is not relevant as neither device nor app communicate any information to internet services. Therefore, we see no privacy issues with the Nemef Entr.

7 BABY MONITORS

Smart baby monitors are a fast growing category in smart devices. The convenience of a well-functioning baby monitor which operates over WiFi and the Internet is much appreciated. This removes the limitation of a wireless signal between the monitor and the base-station, and allows for more information to be provided back to the monitor such as audio, video, temperature, humidity and movement. The monitor device generally allows communication back to the base-station through voice, lights, songs and directing camera devices. As these devices are aimed at use with children they have additional privacy requirements from a GDPR/AVG perspective.

7.1 iBaby Monitor M6

7.1.1 Product description

The iBaby Monitor M6 is a baby monitor with a unique design and extensive functionality. The device has a camera that can be turned 360 degrees using the mobile application. Further, the device can play music as well as transmit audio to and from the baby.

Figure 18: iBaby Monitor M6

The device comes with a concise quick start guide. The website of the manufacturer contains a more extensive manual for both the product and the mobile application.

7.1.2 Security

In order to set up the device, the mobile device with the application must be attached to the iBaby monitor using a USB cable. Then, the WiFi data is shared and the device is ready for use. This ensures that no connection to the device can be made from anyone that does not have physical access to the device.

The data is not sent directly between the device and the mobile phone on which the application is installed. Instead, the device communicates through an external cloud server. In order to make use of the app, users must create an account on which their data is stored. Authentication is required in the form of a username and password combination. The data in transit is encrypted using a TLSv1.2 connection.

Analysis of the communications with external resources showed seventeen unique IP addresses that were accessed. Most of these were accessed over TLSv1.2, however, we observed downloads of firmware and audio files over HTTP.

We successfully performed a Man-in-the-Middle attack. However, we found that some form of certificate verification is in place as the app shows an error that an invalid certificate is being used.

Despite this error, the device did still function (i.e., we could still view the feed and move the camera around).

The device communicates with multiple third-party API's. It is unclear what data is being transmitted.

Upon testing there was no communication over telnet found. Further, we could not determine the credentials to the telnet service.

We found that the device does not update automatically. According to online resources the device can be updated via the settings → version menu, but this option was not available for us in the app. We found no way to force an update on the device. We recommend to further investigate this device, based on this mismatch and the strange certificate verification behavior mentioned earlier.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
Medium	Medium	High	Automatic updates are not supported.
Medium (Medium)	Low	High	(Nessus) Unencrypted Telnet Server.

Table 17: Findings for iBaby Monitor M6

7.1.3 Privacy

There is no specific product Privacy Policy available, but iBaby Labs has published a general Privacy Policy on their website for all apps, products and services offered by iBaby Labs, Inc. (not available in Dutch). This Privacy Policy is based on American law, not GDPR. The latest version was published December 5th, 2014. Updated versions will be published on their website.

The lacking Privacy Policy states that:
iBaby only collects personal identification information from users if they voluntarily submit such information to iBaby. More specifically, this information is name, email address, mailing address and phone number. They do not specify what other data is processed using the iBaby Monitor. For example, iBaby Monitor can make video and audio recordings, but this is not addressed in this Privacy Policy. They mention that iBaby also collects non-personal identification information, which includes browser name, type of computer and technical information. In addition, the operating system and the Internet Service Providers utilized and other similar information. They mention that it is non-personal data, but this data can be linked to personal data from the user. According to the GDPR, this turns this non-personal data into personal data.

Users are not informed of their rights. iBaby mentions they comply with Children's Online Privacy Protection Act, which indicates they do not maintain or collect personal information at their website or apps from children under the age of 13.

iBaby mention they adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of personal information, username, password, transaction information and data stored on their website or apps. Sensitive and private data exchange between website or apps and its users happens over an SSL secured communication channel and is encrypted and protected with digital signatures. Site and apps are also in compliance with PCI vulnerability standards.

Overall, iBaby does not comply with EU laws and regulations. It is undefined exactly which types of data are processed and they misclassify certain data as non-personal. The policy is also out of date. Because of this, the sensitive nature of the device and the fact that all communication passes through a significant amount of cloud services, we conclude that this device has serious shortcomings when it comes to privacy.

7.2 Arlo Baby

7.2.1 Product description

The Arlo Baby is a smart baby monitoring device with an adjustable 1080p camera, audio player, nightlight and air sensors. The monitor is well designed and has a bunny-like appearance. The device also contains a battery, so it can be use cordless for a few hours. A small light on the back of the monitor can be turned on, so it can function as night light.

Figure 19: Arlo Baby

The device works in combination with the Arlo mobile application, which is supported on iOS and Android devices. In order to use the device with the mobile application, a cloud account must be created. Via this cloud account, the camera can also be viewed from a webpage. The camera livestream and recorded videos are transmitted to and stored within the cloud account.

7.2.2 Security

During the installation the mobile application and device can be connected using the wireless access point on the baby monitor. After the initial configuration, the device and mobile application communicate via external servers. We observed connectivity to five resources outside of the EEA. All connections to external resources, besides NTP and DNS, are initiated using TLSv1.2.

Changes in the device configuration are made through the mobile application, for which the user must be signed in. Authentication takes place over a TLS protected communication stream and consists of a combination of username and password. Man-in-the-Middle attempts are blocked by certificate pinning.

Upon installation, the device checks for software and firmware updates. After the initial setup, the device updates automatically.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
Low (Medium)	Low	Medium	(Nessus) SSL Certificate Cannot Be Trusted.
Low (Medium)	Low	Medium	(Nessus) SSL Self-Signed Certificate.
Low (Medium)	Low	Low	(Nessus) SSL Medium Strength Cipher Suites Supported (SWEET32).
Low (Medium)	Low	Low	(Nessus) SSL Weak Cipher Suites Supported.
Low (Low)	Low	Low	(Nessus) SSL RC4 Cipher Suites Supported (Bar Mitzvah).

Table 18: Findings for Arlo Baby

Generally, most of these findings are related to the SSL certificate being signed by an unknown party. After investigating the certificate was found to be self-signed by Netgear, the company behind Arlo. There is no indication that the certificate is vulnerable. However, usage of self-signed certificates is considered a weakness.

7.2.3 Privacy

There is no specific product Privacy Policy, but a general Privacy Policy on the website for all Arlo's products (not available in Dutch). Latest version July 17, 2018. Updated versions will be published on the website and users will be sent a notification.

The Privacy Policy states that:

Personal data is being collected for registration, such as name, country, email, date of purchase. However, they mention that they may also collect additional information such as your interests or hobbies, your gender or age. They do not mention why they want to collect that information. Arlo also collects information you voluntarily share or post, such as information in a public space on their website. You can take videos with this baby monitor and Arlo can email these videos to their users. When personal data is no longer necessary for the purposes for which Arlo processes it, they take measures to delete personal data or keep in it a form that does not permit identifying the person.

Users are clearly informed of their rights. No personal data is being collected from children under the age of 16.

Arlo mentions they maintain administrative, technical and physical safeguards to protect personal information against accidental or unlawful destruction, accidental loss, unauthorized alteration, unauthorized disclosure or access, misuse, and any other unlawful form of processing of the personal data in their possession. They also indicate that they contractually require their suppliers to protect such data from unauthorized access, use, and disclosure.

Arlo's Privacy Policy complies with legal and regulatory requirements. As with other devices, the lack of a specific policy means that it is undefined exactly what data this particular device processes. Additionally, the communications security issues we found may compromise privacy. The observed connections to external resources fall within expected behavior.

7.3 Alecto IVM-100 WiFi Babymonitor with camera

7.3.1 Product description

The Alecto camera looks simple and somewhat cheaply made. Its appearance does not indicate this is a baby monitor. Instead it looks like a basic network camera. Configuration of the baby monitor and further use of it is done using the app (AlectoCam). The app offers very basic functionality. The manual is brief but complete and of decent quality. More information, e.g., regarding the app, is available in additional documentation online.

Figure 20: Alecto IVM-100 WiFi Babymonitor with camera

After connecting the device to a WiFi network with an internet connection, the video feed can also be viewed from remote locations with the app. Without an internet connection the camera can still be used on the local network. It is also possible to insert an SD card to store video recordings.

7.3.2 Security

During the initial setup, the app communicates with the camera via a direct WiFi connection. The communication streams are over TLS. One of the first steps of the setup is to change the default admin password, but this step can be skipped by the user. During the setup the user is required to connect to a WiFi network.

After a connection with a WiFi network has been made, the device is reachable via the internet. To achieve this, the device connects to a cloud-based resource. We observed connections to twelve

resources outside of the EEA, all of which use TLS. We were not able to interpret the communications and thus cannot say to what extent this introduces a risk.

We were informed by the manufacturer that the device checks for firmware updates automatically each night, which is an undocumented feature. We confirmed that this is indeed the case. We found no way to manually check for updates in the app, neither could we influence the automatic update process somehow.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
-	-	-	-

Table 19: Findings for Alecto IVM-100 WiFi Baby monitor with camera

7.3.3 Privacy

There is no specific product Privacy Policy online or in the user manual. At the website Alecto only provide the following information about privacy in the product description (available in Dutch):

- The Alecto APP and the Alecto camera work with a unique UID code, login name and password. No name and address details and / or address are requested or saved from you.
- The secure server only stores the IP addresses and UID of the Alecto camera and smart device for a maximum period of 30 days.
- The server complies with ISO 27001: 2013 (Information Security Management System) and has been verified by BSI & KPMG.
- The server is AWS certified.

Alecto does not comply with EU legal and regulatory requirements in terms of their Privacy Policy. They are not specific and transparent enough regarding the processing of data when using the device. The device communicates with a seemingly unnecessary amount of external servers, including twelve different IP addresses outside of the EEA. All in all, the privacy of this device is insufficient.

8 THERMOSTATS

Thermostats which can be accessed via the Internet are very popular product with consumers. Energy providers are actively promoting the use of these devices. The use of these thermostats provides benefits such as energy use reports. This provides consumers insight in electricity and gas consumption. The thermostats also provide ease of use capabilities for the consumer to remotely adjust the configured temperature.

8.1 Nest Learning Thermostat V3

8.1.1 Product description

The NEST learning thermostat V3 is a smart thermostat to control home heating systems through OpenTherm. The device has a simple elegant design and is very responsive and user friendly.

The thermostat is connected via WiFi and communicates with a cloud-based service. The device can be controlled physically, as well as remotely via the mobile application or NEST website.

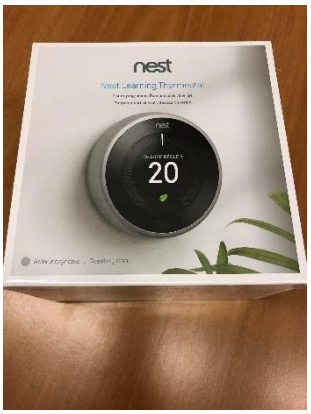

Figure 21: Nest Learning Thermostat V3

8.1.2 Security

During the installation of the device, a WiFi connection is set up. The WiFi connection is required in order to use the device. While linking the Nest with a mobile device, a pairing key is generated by the Nest which must be filled in on the mobile device. This ensures that no-one without physical access to the device is able to link to the device.

All communication takes place via a cloud service. We observed connections to twelve different IP addresses outside of the EEA, all of which use a TLSv1.2 connection. Additional security controls allow users to configure a 4-digit PIN on the device to prevent unauthorized control. Also, users can configure two-factor authentication for their cloud account. Updates are installed automatically on the Nest.

After performing a vulnerability scan, only informative findings were returned by the scan. In addition, the port scan did not return any open ports with services that could be exploited.

The device is automatically updated when it is connected to WiFi.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
-	-	-	-

Table 20: Findings for Nest Learning Thermostat V3

8.1.3 Privacy

There is a Privacy Policy for all Nest products on Nest website, some specific provisions for this product (available in Dutch). Changes of the Policy will be published on the website and Nest notifies its users. The latest version is from September 24, 2018.

The Privacy Policy states that:

Nest will provide a detailed description of what personal data is collected and for what purposes. Nest collects setup information users provide, environmental data from the Nest Learning Thermostat's sensors, direct adjustments to the device, heating and cooling usage information and technical information from the device. Within the Privacy Policy all these descriptions are very detailed.

Nest uses all the personal data they collect to provide, develop and improve the product and services. They use aggregated user data for research purposes.

Users are clearly informed of their rights. Nest states they do not collect personal data of children under the age of 13 and only people from the age of 18 and older may act as the owner of Nest accounts. Authorized users must be over 13 years old or the equivalent minimum age in the jurisdiction where they are located.

Nest mentions they use best-in-class data security tools to keep personal data safe and protect the Nest Products from unauthorized access. Personal data from Nest devices is encrypted while it is being transmitted to Nest.

We have no issues with Nest's Privacy Policy. It is very comprehensive. In addition, the only aspect that may compromise the privacy of the user is the large amount of cloud resources that are accessed.

8.2 Nefit ModuLine Easy

Figure 22: Nefit ModuLine Easy

8.2.1 Product description

The Nefit ModuLine Easy is a smart thermostat with a nice glass design. It feels solid and heavy. Its controls are more basic than comparable smart thermostats and the screen is smaller than the other devices. The included manual is short but covers all the necessities. It is rather old (2015/06) but no irregularities were found. An appendix is included for used open source components and is only available in English.

During the initial configuration the device is connected to a WiFi network. After connecting, the device can also be managed through an smart app. A QR code is included on the manual which is needed to add the thermostat to the app.

8.2.2 Security

After connecting the thermostat to the WiFi network, a manufacturer-hosted resource is resolved via DNS. The thermostat then sets up an XMPP session over TLS with that resource. We established a Man-in-the-Middle with a self-signed certificate on this connection and were able to extract a DIGEST-MD5 challenge-response sequence. The username that is used for the connection can be extracted from this, but we were unable to crack the password by using a 1.2 billion words dictionary attack. Besides this connection to the manufacturer-hosted resource, we observed connections three resources outside of the EEA, two of which are DNS resources. The other resource is accessed using a TLSv1.2 connection, over which no significant amount of data is transferred.

When the app connects to the thermostat, all communication is also done over this XMPP channel. Further analysis of the communications stream indicates that the commands that are sent to the thermostat are encrypted in some way as well.

The manual and website state that the device should be automatically updated. We did observe version checking in the XMPP communications, however no updates were witnessed in the monitored communication.

When opening the app, a HTTP POST request is made to another cloud hosted REST API. Since it is an unencrypted HTTP request, we were able to extract an API key. We assume that the response that is given to the initial request is required to update the commands the app uses. Further analysis of what would be possible with the extracted API key is out of scope for this project. We recommend to further investigate this.

The device is automatically updated when it is connected to WiFi.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
Medium	Medium	Medium	Information disclosure through unencrypted REST API.
Low	Negligible	High	No certificate pinning in the mobile app.
Low	Low	Low	Offline password cracking due to DIGEST-MD5 authentication.

Table 21: Findings for Nefit ModuLine Easy

8.2.3 Privacy

Nefit provides a detailed general Privacy Policy for their website and mobile application (available in Dutch). In addition, they provide details regarding data processing for the Nefit Moduline Easy. The Policy is dated 24th May, 2018. Updated versions will be published on the website and users will not be notified of any changes.

That said, one of the advantages of this device is that the data is not stored in the cloud. Everything is stored in the device itself. Nefit states they only needs personal data for warranty, maintenance and maintenance work and for service purposes, but not for the use of the product. All data required for the proper functioning of this product is constantly stored in your product itself. When using the apps, all data is stored in your mobile device. These can only be viewed and used with a user's personal access code. Nefit has no access to personal data. Users can give permission to access the data in the product, but they can revoke this access by turning it off in the app.

Nefit states takes the necessary security measures to protect personal data managed by Nefit against manipulation, loss, destruction, access by unauthorized persons or making unauthorized public. They mention their security measures are constantly being improved in accordance with technological developments.

Nefit's Privacy Policy complies with legal and regulatory requirements, especially in combination with the further details specified on the website. We see communication streams to external servers that we do not know the purpose of. We cannot be certain the purpose of this data is consistent with the purposes specified in the policy.

8.3 Remeha eTwist

Figure 23: Remeha eTwist

8.3.1 Product description

The Remeha eTwist is a smart thermostat with a simple design and intuitive controls. Additional functionality allows the user to change the temperature based on the room and weather, as well as providing insight in energy usage.

During the initial configuration the device can be connected to a WiFi network. It is not required to do this if the device will only be used locally. However, in order to control the device from any location the app must be used, for which WiFi and registration via the app is required.

Both the included user manuals and gateway installation manual are available in Dutch.

8.3.2 Security

As the Remeha eTwist does not need to be connected to WiFi, many potential security threats can be mitigated if the user wants to. However, doing so takes away functionality that separates a smart thermostat from a normal thermostat.

After connecting the thermostat to the WiFi network it can be used with the mobile eTwist application for which registration is required. In order to connect the device and the mobile application, the thermostat generates a QR-code which is displayed on the screen. The user can scan this QR code with his mobile device to link the mobile device and the thermostat. This means that physical access to the thermostat is required in order to connect a new mobile device.

The communication between the device and mobile application runs through an external server. Remarkably, communication between the mobile application and the external server runs over a TLSv1.1 data stream, whereas the communication between the external server and the thermostat itself run over a TLSv1.2 data stream. Connections to external resources outside of the EEA were observed, but these are only NTP services.

The device is automatically updated when it is connected to WiFi.

The following table summarizes our findings as well as the Nessus scan results.

Risk (Nessus)	Probability	Impact	Description
Low	Low	Low	Outdated TLSv1.1 connections.

Table 22: Findings for Remeha eTwist

8.3.3 Privacy

Remeha publishes a product Privacy Policy on the website (available in Dutch), both a summary and a link to the full version. The latest version is from November 13, 2017. Updates versions will be published on the website and users will be sent a notification.

The Privacy Policy states that Remeha provides a very detailed description of what personal data is collected and for what purposes. Remeha only collects the necessary personal data for the provision of services and contact with the customers. Aggregated data is processed to improve products and services. Some personal data is processed directly or stored in the smart thermostat or the app. Users can remove such personal data by resetting the thermostat to the default settings or by removing the app.

Users are clearly informed of all their rights.

Personal data is stored in Remeha systems as long as it is necessary for the purposes described in the Privacy Policy, or to the extent that it is necessary to comply with all legal obligations and to resolve disputes. If users delete their account or if Remeha no longer needs the personal data, Remeha will delete or anonymize the data.

Remeha mentions that they take the necessary technical and organizational measures to ensure that personal data is well protected and therefore protected against unauthorized or unlawful use, modification, unauthorized access or disclosure, unintended or unlawful destruction and loss.

Remeha's Privacy Policy complies with legal and regulatory requirements. Our findings with respect to communications security may pose some risk to privacy.

9 IOT DEVICE SCORE

The table below provides an overview of the overall score each individual IoT product within each of the defined categories. Scoring is based on the conducted assessments of the devices, according to the scripts described in Chapter 2. Devices are scored based on a curated list of security aspects from the testing script, where each aspect contributes a certain amount of points. The overall score is given as a percentage of the maximum possible score. As we noted in Chapter 2, devices should primarily be compared to devices within their own category. A device with a high score is not necessarily "safe". devices with a single critical finding can still have a relatively high score but be insecure at the same time. Establishing a simple and understandable benchmark of safety for IoT devices is very much still an open problem.

Product	Category	Score %	Most severe finding
TP-LINK ARCHER C3150	Routers	**71,0%**	Medium
Huawei B315s-22	Routers	**82,8%**	Medium
Linksys MAX-STREAM EA7500	Routers	**73,1%**	Critical
Asus RT-AC68U	Routers	**78,8%**	Medium
Netgear Nighthawk X4S R7800	Routers	**78,2%**	Medium
VTech Storio Max	Smart Toys	**79,2%**	High
Spider-Man App-Enabled Superhero	Smart Toys	**79,5%**	Low
MAKEBLOCK Codeybot	Smart Toys	**53,8%**	Critical
RC Spy tank met camera	Smart Toys	**45,3%**	Critical
I-Spy Tank met camera - RC Tank	Smart Toys	**43,7%**	Critical
Ubiquiti UniFi Video Camera G3	IP Cameras	**75,5%**	Medium
Foscam C1	IP Cameras	**74,4%**	High
Hikvision DS-2CD2385FWD-I	IP Cameras	**77,5%**	Medium
Nuki Smart Lock	Smart Locks	**69,2%**	High
Danalock V3 Homekit	Smart Locks	**74,5%**	High
Nemef Entr	Smart Locks	**82,5%**	Medium
iBaby Monitor M6	Baby Monitors	**78,7%**	Medium
Arlo Baby babyfoon	Baby Monitors	**85,8%**	Low
Alecto IVM-100 wifi babyfoon met camera	Baby Monitors	**80,7%**	No findings
Nest Learning Thermostat V3	Thermostats	**87,4%**	No findings
Remeha eTwist	Thermostats	**79,1%**	Low
Nefit ModuLine Easy	Thermostats	**78,4%**	Medium

Table 23: IoT Device Score

10 DISCUSSION

This chapter focuses on a discussion of the first of our research questions: “How secure is the software on popular consumer IoT devices?”

As we indicated in the introduction, we have looked into the first question in terms of existing vulnerabilities, insecure or unused services, access control, firmware upgrades and more generally in terms of adherence to security and privacy by design principles.

The design principles of most consumer devices have a focus on meeting the required features as quickly as possible to reduce the cost of development. Security by design and privacy by design introduce additional cost in development. The balance between development cost optimization and security/privacy design considerations depends on the sensitivity of the collected data, and the impact of the device on its environment. Routers are, for instance, internet-enabling devices for among for, e.g., financial transactions, require a high level of security by design. Locally connected toys which are unable to record any relevant data have lower requirements.

10.1 Routers

Routers have been around for a long time and are generally mature and well-developed products in the assessment. Routers are also the most complex and provide the largest attack surface. A compromised router makes further attacks on other devices in the network a lot easier. It is therefore crucial that the security of these devices is set up properly.

In terms of security the routers generally have similar issues.

- Insecure authentication. In particular they all use HTTP by default. Some routers attempt to get around this by implementing client-side parameter encryption schemes that do not reveal the credentials even when using HTTP. Others use simple plaintext or base64-encoded credentials, which an attacker can steal.
- Insecure default services like FTP, UPnP or Telnet. In particular, for both FTP and Telnet the communication can be eavesdropped. UPnP, when enabled by default, is a well-known security risk as well.

The tested routers all prompted the user to change the password during initial configuration. On the other hand the credentials are often transmitted between the browser and the router in plain text.

All of the tested routers have adequate privacy policies in place and comply with the legal and regulatory requirements. Some routers use poor authentication practices, leaking credentials in the process. This allows an attacker to take control of the router and subsequently monitor the entire network. This allows for unauthorized collection of personal data transmitted on the local network.

10.2 Connected toys

Smarts toys are a very diverse category of devices. The devices we tested range from almost fully functional (but child-proofed) android tablets to mobile-app-controlled camera-equipped miniature cars. Many of the devices tested are wireless access points with additional functionality. Interaction with the device is done by connecting to access point and then controlling the device with the mobile application. This reduces the potential threat of insecure toys, since the device and the app are not on an internet connected networks. It must be mentioned that mobile devices are often themselves connected to the internet through 3G/4G, which poses an indirect security threat.

In terms of security the connected toys fall on the extreme ends of the spectrum. Two of the devices tested performed well with no detected flaws. Three devices are insecure. The wireless access points used no authentication or encryption. This allowed us to fully control these devices from anywhere within wireless range.

In terms of privacy, two of the devices lack any Privacy Policy whatsoever. This corresponds directly with the devices that were insecure. The other three devices have adequate Privacy Policies in place, with no major privacy risks found.

10.3 IP Cameras

An IP camera is a camera connected to the network, through either ethernet, WiFi or both. They are an attractive target due to the potential for spying or reconnaissance. They are used in both home and business environments and generally feature very similar functionality.

For IP cameras it is absolutely critical that users update the devices. Many of the tested devices have known vulnerabilities for older version that have since been patched. In addition, communications security is still lacking after the updates. Plain HTTP is still used sometimes and even if TLS is employed, it is outdated or misconfigured.

In terms of privacy, the published policies are all adequate and compliant with laws and regulations. However, the aforementioned communications security or authentication issues may still pose a threat to privacy.

10.4 Smart Locks

The tested smart locks were in many ways very similar. All employ Bluetooth for app-to-lock communication, all have other physical ways of (un)locking the device and all are mounted on the inside of a door. They also share similar features, like automatic (un)locking. Security is obviously critical for a lock, in particular since these locks will often be attached to front doors.

All tested locks seem fairly secure from a software and implementation perspective. Classic Bluetooth replay and sniffing attacks fail and the mobile applications seem well-hardened. However, relay attacks, where an attacker relays the signal from a legitimate mobile device to the lock, are still possible for some locks. Physical security is another real issue that plagues these smart locks. Often, the default settings allow very easy manual (un)locking. For instance, by pressing a button. While very convenient, and good in terms of escape in case of emergency, any door that allows some kind of access to the interior can expose this behavior from the outside. A simple letterbox is probably enough and would allow an attacker to unlock a door from outside with simple equipment.

In terms of privacy, the policies still leave some facts regarding data processing uncertain. However, as these devices have very little or no communication to external servers they do not seem to pose a privacy risk.

10.5 Baby Monitors

Baby monitors have a lot in common with IP Cameras from a technical perspective, though they generally offers slightly different feature sets. In particular, the baby monitors generally include a speaker that can play audio. In terms of security risks, baby monitors share many of them with IP cameras. That said, they also are intended to monitor babies and small children, which heightens the threat of insecure devices and introduce more stringent demands regarding privacy.

In terms of security, none of the devices are easily exploitable. However, all tested baby monitors have issues with either insecure protocols or an outdated, misconfigured TLS setup.

The Privacy Policies for the baby monitors are severely lacking, with one exception. We found them to be outdated, incomplete or not applicable to EU laws and regulations. In addition, the privacy risks are exacerbated due to the lack of communications security and the sensitive nature of the data being processed.

10.6 Smart Thermostats

Smart thermostats can reveal a lot of information about the residents of a home they are installed in. Most notably, they can often detect when people are at home. In addition, there are definite health risks associated with an attacker gaining control over a thermostat.

In general, the tested smart thermostats were mature from a security perspective. Software updates are all automatic, communication is encrypted and access control is suitably in place. For some thermostats, however, there are issues regarding outdated protocol versions, making the aforementioned encryption and access control a lot less secure.

In terms of privacy, the published policies are all adequate and compliant with laws and regulations. While the aforementioned security issues may introduce some risk, overall these devices pose little risk.

10.7 Overview

In general, the IoT devices tested during this assessment show some definite patterns in terms of security issues. By far the most common issue regards insecure, outdated or misconfigured communication protocols. Usage of plain HTTP is prevalent and so is the usage of either old and vulnerable TLS versions. Secure certificate handling (certificate pinning, CA pinning, etc.) is also not universally implemented, though it is increasingly common.

Note that there are reasons for not using TLS on local web configuration interfaces. Many IoT devices, if they support configuration through web browsers, would yield HTTPS browser errors because of hostname errors in the certificate. Advising users to simply ignore such warnings creates bigger problems than it solves. Given the ability to change the certificates on a device, a knowledgeable user can circumvent this issue. However, for general consumer usage we see no generic solution. Still, some encryption is better than no encryption at all.

Though many devices still come with default passwords, the user is almost always prompted to change this during initial configuration. That said, if that same password is then transmitted over HTTP it really defeats the point.

In terms of security by default, default configurations often prioritize convenience and compatibility over security. Additionally, unused or insecure services/ports are often left open. While this does not always pose a security risk per se, this does needlessly increase the attack surface. It also makes securely using a device more difficult, since a user has to go through a number of steps to enable security features. In particular, updating firmware on IoT devices is often a relatively complex, yet absolutely necessary step towards securing the device.

When it comes to privacy, we find there is a lot of uncertainty regarding what data is actually processed by a specific device. In large part this is due to the lack of a specific Privacy Policy. Those devices where a specific policy is available provide a lot more clarity as well as trustworthiness and accountability. The lack of a specific policy also leads to very broad Privacy Policies where the purpose processing data is often very generic and broad as well. As we noted before, lacking security practices also have a significant impact on privacy.

11 RECOMMENDATIONS

In this chapter we provide some recommendations for minimum security requirements for IoT devices. As we noted in the previous chapter, there are definite patterns where IoT security problems are concerned. Our recommendations follow naturally from those patterns and they often relate directly to either security or privacy by design.

11.1 Security requirements

For our recommended requirements we focus on security aspects that closely correspond to the patterns we discussed in Section 10.7:

- Security of communications
- Unused or insecure services
- Authentication
- Usability

Many of the recommendations we make directly relate to security by design in that they recommend better, more secure defaults, reducing attack surface and overall making the security features easier to use.

11.1.1 Security of communications

Across categories we have seen poor use of communications security. Secure communication protocols are either not used at all or badly used. Where possible at we would like to see the following things implemented as a minimum baseline:

- Use secure communication protocols everywhere. Often this means using protocols based on either TLS or SSH. Plaintext communication is almost always a red flag.
- Just enabling secure protocols is not enough, they have to be set up correctly too. For TLS this means using current protocol versions, certificates that actually validate, implementing certificate and/or CA pinning and using modern, secure cipher suites. The converse of this that insecure protocols and options must be actively disabled.

11.1.2 Unused or insecure services

As it is important to bring the attack surface of a device to a minimum, we recommend that unused services are simply disabled or otherwise made inaccessible. Going a little further, device manufacturers could publish the list of enabled services that are necessary for device functionality. This may help users with limited technical knowledge to understand what services are required and which services could potentially be turned off to increase their security. We saw evidence of this in a few manuals, but this is by no means a common practice.

As for insecure services, they should be disabled or replaced by secure alternatives. In our considered opinion there are no good reasons to use something like Telnet instead of SSH. This strongly relates to our earlier point about using secure communication protocols.

11.1.3 Authentication

As we noted earlier, vendors seem to have adopted better password standards in the last few years. They are either randomly generated or forcibly changed during initial configuration. As a minimum, either option should be a requirement. Users should also be encouraged to choose secure passwords, with a focus on password length and uniqueness as indicators of security.

11.1.4 Usability

There is often tension between usability and security. Making something more secure often makes it less user-friendly as a result. That said, it is crucial that securing a device is as easy as possible. A lot of this is accomplished by providing secure options by default.

A more specific example is enabling automatic updates. If implemented securely, automatic firmware updates ensure that users no longer need to worry about keeping their devices updated. This does absolutely require that the firmware update is implemented securely. That means, at a minimum, using secure communication protocols and implementing integrity checks through cryptographic signatures on firmware updates.

11.2 Privacy requirements

For our recommended privacy requirements we consider both the legal and regulatory requirements that devices already have to comply with as well as possible additions or clarifications.

- For each specific device there must be a clear Privacy Policy stating which personal data is being processed and for which purpose. The user must be informed about the processing of personal data, to comply with the GDPR principle of transparency. The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand. Transparency helps to establish trust in IoT device security and privacy.
- Devices should adhere to principles of privacy by design. Functionality that may affect the privacy of the user should be opt-in where possible. Often, the core features of a given device do not require personal data to function. Such data should not be process “just in case”. This also relates to the principle of data minimization.
- Whenever personal data is being processed users should be aware of this. Users should be in control of their personal data that is being processed and have the ability to exercise their privacy rights.

11.3 Recommendations for using IoT devices

Besides our recommendations for minimum security requirements for IoT devices, we stress the importance of correct usage of IoT devices by their users. Even if a device complies with all security standards and requirements, incorrect configuration or incorrect usage of the device can increase the chance of potential vulnerabilities. Principles of security and privacy by design and default are supposed to mitigate this risk. However, until such time as these principles become the de facto standard, correct usage of IoT devices is still of critical importance.

We therefore have a number of recommendations for using the tested devices:

- Ensure devices are regularly updated, preferably using automatic updates (if supported). Security patches, aimed at fixing or disabling vulnerable services, are regularly delivered to IoT devices via software updates. Therefore, it is important to install these updates regularly and as soon as possible.
- Whenever a device uses a default, not randomly generated password, we strongly recommend changing the password. Ensure this password is secure by using a long passphrase or a password generated by a password manager. If possible, we recommend using multi-factor authentication. However, we did not see many IoT devices supporting any kind of additional authentication methods.
- Segregating possibly untrusted IoT devices on their own networks if possible. This may be a little more advanced for average users but it goes a long way to mitigating the risk of using IoT devices.
- Limit the extent of personally identifiable information on the device to as little as needed and ensure that sensitive (personal) information is removed.

12 CONCLUSION

Both IoT device security and privacy are increasingly important as more and more IoT devices enter the market. In order to ascertain the state of security and privacy in IoT we performed an assessment of 22 IoT devices available on the Dutch market. This assessment focused on the following research questions: Firstly, “How secure is the software on popular consumer IoT devices?”. In particular, we considered adherence to principles of “Security by Design/Default” and “Privacy by Design/Default”. From there, we answered the second research question: “What should be the minimum security requirements for IoT devices?”

We provide detailed answers to these questions in Chapters 10 and 11 as well as in the individual device reports. Overall, many devices performed better than we may have expected in terms of security. Better does mean good, however. Across the board we found many cases regarding outdated and/or misconfigured communications security. We saw a number of devices using insecure services or leaving unused services available. There were a few devices that had very poor security, primarily in the connected toys. On a happier note, smart locks in particular have improved their level of security in the last few years. As we noted in the introduction, in 2016 there were still a lot of problems in this category, most of which we cannot reproduce on the current crop of devices.

In general, we found that four of the 22 devices had findings that were classified as ‘critical’. Respectively four and nine of the devices had findings for which the severity was ‘high’ or ‘medium’. Only for two of the devices we did not have any findings at all.

In terms of privacy there were some devices that did not comply with EU laws and regulations, as they have an insufficient or nonexistent privacy policy. Additionally, insufficient communications security is a risk to privacy irrespective of the official policy. We also observed that many devices connect to external servers, often outside the EEA. While some, or even most, of this behavior is done for legitimate reasons, it does raise questions as to what data is being communicated and for what purposes.

Our recommendations follow naturally from our findings. At a minimum we want to see secure communication protocols used everywhere and insecure or unused services disabled or replaced. Security features should be either enabled by default or very easy for a user to enable. Similarly, features that either compromise security or collect personal information should be opt-in if they are not essential to the core functionality of the device.

A number of devices had findings that, due to constraints on the time and the scope, were not further investigated. As such, we recommend further investigation of two devices specifically. First, the Nefit ModuLine Easy, for which we were able to extract an API key, the usage of which to explore the API was out of scope. Second, we recommend further investigation of the iBaby Monitor M6, as the device communicates with a large number of external parties and downloads firmware over HTTP, which may prove exploitable after further research.

ANNEX A: IOT DEVICE LIST

The device list below provides an overview of the individual IoT products tested. It also notes the use of a smartphone App and the Operating Systems supported.

Device Category	Vendor and Device Type	Device software version	Smartphone App	Android version	iOS version
Routers	Huawei B315s-22 Wit	21.329.01.00.983	Optional	4.3+	8.0+
	TP-Link Archer C3150 v2.1	2_170926	Optional	4.3+	9.3+
	Linksys MAX-STREAM EA7500	2.0.7.191563	Optional	4.1+	9.0+
	Asus RT-AC68U Zwart	384.10_2	Optional	4.3+	9.0+
	Netgear Nighthawk X4S R7800	1.0.2.62	Optional	4.2+	9.0+
Connected toys	VTech Storio Max Roze - Kindertablet	62.ETV5C	Yes	4.4+	7.0+
	Spider-Man App-Enabled Superhero	3.8.2 / 20170824	Yes	4.3+	9.0+
	MAKEBLOCK Codeybot Wit	1.0.0	Yes	4.0+	7.0+
	RC Spy tank met camera (attop)	Unknown	Yes	2.3+	6.0+
	United Entertainment - I-Spy Tank met camera - RC Tank	Unknown	Yes	1.6+	4.3-10
IP Cameras	Ubiquiti UniFi Video Camera G3 (1-pack)	4.8.40	Yes	4.3+	10.0+
	Foscam C1 Zwart	1.12.5.4_2.82.2.33	Yes	4.1+	8.0+
	Hikvision DS-2CD2385FWD-I	5.5.80	Yes	4.1+	8.0+
Smart Locks	Nuki Smart Lock	1.7.3	Yes	4.4+	10.0+
	Danalock V3 Homekit	0.10.3	Yes	5.1+	9.0+
	Nemef Entr	B1.2.2b396M16.06b1N6.4F160919.0	Yes	4.3+	8.0+

Baby Monitors	iBaby Monitor M6	5.2.0	Yes	4.1+	8.0+
	Arlo Baby babyfoon	1.8.6.2_22781	Yes	5.0+	10.0+
	Alecto IVM-100 wifi babyfoon met camera	41.0.2.163	Yes	4.1+	8.0+
Thermostats	Nest Learning Thermostat V3 (Zilver)	5.9.3-6	Yes	Differs per device	10.0+
	Remeha eTwist	1.53.2	Yes	4.3+	8.0+
	Nefit ModuLine Easy	02.19.01	Yes	4.0+	9.0+

Table 24: IoT device list

Remarks:

Latest smart phone OSes used at the moment of writing this document:

(The 32/64 bit CPU used within the IoT device determines which latest software release can be used).

Android : 9.0 (August 2018)

Apple : 12.2 (March 2019)

ANNEX B: ABBREVIATIONS

API	Application Programming Interface
AVG	Algemene Verordening Gegevensbescherming
AWS	Amazon Web Services (Cloud Service)
CBC	Cipher Block Chaining
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
DHCP	Dynamic Host Control Protocol
DNS	Domain Name Service
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
MAC	Media Access Control
PCI	Peripheral Component Interconnect
iOS	iPhone OS (Apple)
ISO	International Organization for Standardization
LAN	Local Area Network
MitM	Man-in-the-Middle (attack)
OS	Operating System
PIN	Personal Identification Number
RSA	Public-key Encryption named after Ron Rivest, Adi Shamir and Len Adleman
RTSP	Real Time Streaming Protocol
SMB	Server Message Block
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
UPnP	Universal Plug-and-Play
UID	User Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
WiFi	Wireless Fidelity
WPA2-PSK	WiFi Protected Access 2 – Pre-shared Key
XMPP	Extensible Messaging and Presence Protocol
XSS	Cross Site Scripting