TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technology

TTU IT College

Oliver Erlich 192910IVSB

Consumer Grade IoT Security Analysis: a Case Study

Bachelors' thesis

Supervisor: Mohammad Tariq Meeran
PhD

Tallinn 2022

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

TTÜ IT Kolledz

Oliver Erlich 192910IVSB

Tarbijaklassi asjade interneti turvalisuse analüüs: juhtumiuuring

Bakalaureusetöö

Juhendaja: Mohammad Tariq Meeran
PhD

Tallinn 2022

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Oliver Erlich

16.05.2022

Abstract

Surveillance IoT devices are very common in many homes, but no analysis of security has been done for such cheap consumer IP cameras, whereas only comparative reviews exist where features are closely inspected. Such is the case for Xiaomi Home 360 and Vimtag PTZ 720p as well. It is important to understand the security of these devices because they are cheap and easily accessible to consumers.

To understand the security levels of these devices, certain vulnerability scanning, and analysis must be done, such as port scanning, network traffic monitoring and web application vulnerability scanning. These methods have been previously used in similar case studies. The findings of these experiments are mapped to OWASP Top 10 vulnerabilities, which in turn provide a good security baseline understanding.

Results show evidence of vulnerability in the ecosystems of the devices, lack of physical hardening and insecure data storage. The findings support further research into these devices while completing the goals of the thesis.

This thesis is written in English and is 37 pages long, including 6 chapters and 9 figures.

Annotatsioon

Tarbijaklassi asjade interneti turvalisuse analüüs: juhtumiuuring

Asjade interneti jälgimisseadmed on väga populaarsed tarbijate seas üle maailmselt, kuigi turvalisuse analüüse soodsama klassi IP kaamerate kohta ei ole tehtud. Selle asemel on tarbijatele suunatud võrdlevad ülevaated seadmetest, kus keskendutakse seadmete üldnäitajatele. Vastav kirjeldus sobib ka seadmetele Xiaomi Home 360 ning Vimtag PTZ 720p.

Tähtis on mõista nende seadmete turvalisuse taset, kuna need on soodsad ning lihtsasti kättesaadavad tarbijatele. Turvalisuse taseme mõistmiseks on vaja teha eksperimente ning analüüse, sealhulgas portide skänneerimist, võrguliikluse monitoorimist ja veebiapplikatsiooni haavatavuse skänneerimist. Vastavaid meetodeid on varasemalt kasutatud sarnastes turvalisuse analüüsides. Leitud haavatavused ning analüüsitulemused kaardistatakse OWASP Top 10 asjade interneti haavatavuse nimekirja järgi, mis annab hea ülevaate üldturvalisuse tasemest juhtumiuuringu seadmete kohta.

Tulemused koosnevad asjatõenditest haavatavuste kohta seadmete ökosüsteemidest, ebapiisavast füüsilisest kaitsest ja ebaturvalisest andmete käitlemisest. Leiud toetavad edasist uurimist teemasse, kuigi samal ajal täites lõputöö eesmärgid.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 37 leheküljel, 6 peatükki, 9 joonist.

Table of Contents

List of figures

Background information, abbreviations

Attack vector	a vulnerability, that could be exploited for malicious use.
Botnet	a collection of infected devices used to collectively perform a task or an attack on a target.
DDoS	Distributed Denial of Service, a type of attack used to disrupt or slow a service/site.
DHCP	Dynamic Host Configuration Protocol, a protocol used within routers to attempt automatically assigning IP addresses from a predefined pool of addresses to a newly connected device.
GDPR	General Data Protection Regulation, European Union regulation regarding data protection.
IoT	Internet of Things, smart devices that are network connected.
IP address	Internet Protocol address, an address used within a network to allow for communication, segmentation, grouping.
MAC address	Media Access Control address, unique address for a network interface controller, used for communications within a segment.
Mi Home	the application used to manage and control the Xiaomi Mi Camera.
Monitor Mode	a mode in Wireshark, which has the network card look at surrounding Wi-Fi signals, capturing packets.
SSH	secure shell, network protocol used to securely communicate over unsecured networks.
TCP/UDP	Transmission Control Protocol and User Datagram Protocol respectively, two most common network traffic protocols.
Threat actor	anyone who has potential to impact security, whether unknowingly or knowingly, maliciously.

1 Introduction

The world of Internet of Things (IoT) is becoming larger and cheaper each year, allowing consumers to purchase, own and operate these devices. A 2019 study shows based on scans from 15.5 million homes that 71% of households in North America, 25.7% of households in Eastern Europe and 57.2% of households in Western Europe have at least one or more IoT devices, the global median being 40.2% [1], which shows wide adoption of IoT devices in private homes. As these devices are cheap and accessible to the average consumer, the more interest lies in the security aspect of them.

Increased usage of IoT devices in homes exposes the user to more attack vectors in case of targeted attacks or can serve as a slave within a botnet, playing a role in coordinated attacks like the 2016 Mirai botnet, which infected hundreds of thousands of IoT devices and later exploiting them to coordinate the largest DDoS attack ever seen [2].

The purpose of this thesis is to conduct security assessment of two consumer grade budget IP camera devices, and then to explore and expose any internal or external possible vulnerabilities in a network. Such a security assessment does not exist for these two devices, while being cheap and accessible to consumers. Two devices were chosen for possible comparative analysis. The Xiaomi IoT stack is a very cheap consumer grade IoT solution base, which supports easy setup and usage. Similar can be said about the Vimtag, although a smaller and less known IoT stack. Xiaomi is also a known brand globally, which inherently increases trust within consumers, while Vimtag is a less known brand. This might create a false sense of security in the eyes of the consumer when choosing a product based on all consumer expectations.

It is necessary to review the technical and non-technical security aspects to fully understand if brand reputation and the level of security are correlated or not. Data collection and analysis of security aspects are required to finally understand the actual level of security present with this device.

This thesis aims to answer the question of what vulnerabilities exist for these devices. To answer this question, methods such as network traffic monitoring, port scanning and web

application vulnerability scanning are used. These methods are chosen due to usage in similar articles and works assessing similar situations.

By conducting the experiments and mapping found vulnerabilities to the OWASP Top 10 list, the results show evidence of vulnerabilities found from insecure ecosystems, lack of physical hardening and insecure data transfer and storage. Moreover, no blatant evidence of vulnerability is found from the generated network traffic nor insecure services, such as Telnet or FTP. Possible future research includes further firmware, operating system and web application-based vulnerability scanning and security assessing, where necessary cooperation with the manufacturers is agreed.

The author's goal is to thoroughly analyze the smart camera devices, understanding their operations, communications within the home network and externally, analyze their security level, creating a complete report on the findings.

2 Literature review

According to the International Telecommunication Union [3], IoT is defined as a global infrastructure for the information society, enabling advanced services by interconnecting things based on existing and evolving information and communication technologies. This infrastructure offers services to every kind of application, while attempting to provide and conform to security and privacy requirements set by different regulatory and standardization processes.

IoT security devices can increase home security by providing sensors and optics for monitoring, but they also increase the potential attack surface of homes. The IEEE Consumer Electronics Magazine published an article [4], where it is discussed how these attacks can happen on the physical, network or application layers. These consumer market devices may often compromise on security measures to keep up with market needs, focusing more on time-to-market and minimizing costs. Vulnerabilities for many different devices have been analyzed, including smart thermostats, wearable smart watches, electric vehicle chargers, drones, cameras, televisions, etc. Vulnerabilities such as device hardware exploitation, malicious code injection, device software failure and more have been tested and performed on these devices.

With the introduction of privacy laws such as GDPR, privacy issues of the larger IoT stack have been analyzed in a recent study in the Bleking Institute of Technology [5], whether these devices and technologies conform to the new laws. Case studies have shown compliance, although to different extents. In such case studies, different IoT cameras have been analyzed, although with a focus on information security and privacy. The selection of cameras does include consumer budget devices, although without comparative analysis. The study uses a selection of tools to analyze the security of IP cameras, which include OWASP ZAP, Nmap and Wireshark. OWASP ZAP can be used for scanning web interfaces of these devices, Nmap can be used for network scanning, analyzing responses from devices and Wireshark allows for analyzing network traffic/packets.

Past large-scale attacks, such as the 2016 Mirai malware infected hundreds of thousands of IoT devices, later exploiting them for a large-scale DDoS attack, the size of which was unseen

before [2]. Since then, IoT devices have become even cheaper and more accessible to consumers, increasing the amount of IoT devices within households all around the world [1].

After the 2016 Mirai attack, there has been an increase of studies related to IoT security, specifically about loopholes and flaws within IoT networks [6]. Often, if focused on the security of the network, there is no deep dive into one specific device.

Different IoT devices provide different metrics and information. Devices such as smart light switches don't expose the surrounding environment as much as devices such as IP cameras, which if exposed, provide a threat actor with vision inside a perhaps secure environment. A scan conducted in millions of homes in an analysis of IoT devices in home networks [1] shows widespread usage of IoT surveillance devices, such as IP cameras, in home networks across the world, as shown in Figure 1. These surveillance devices are most common in South and Southeast Asia, where scanning shows 54.5% and 37% of all devices scanned to be surveillance devices in homes.

	IoT	Media/TV		Work Appl		Gaming		Voice Asst.		Surveil.		Storage		Automat.		Wearable		Other IoT	
Region	Homes	Homes	Devices	H	D	H	D	H	D	H	D	H	D	H	D	H	D	H	D
North America	71%	42.8	44.9	32.7	28.0	16.0	12.0	9.5	7.5	3.9	3.7	2.7	1.7	2.3	1.9	0.2	0.1	0.4	0.2
South America	34.4%	20.5	51.7	7.5	24.0	4.3	9.8	0.1	0.3	4.6	13.3	0.3	0.6	0.0	0.1	0.0	0.1	0.1	0.2
Eastern Europe	25.7%	16.8	50.2	6.0	23.6	2.7	7.6	0.2	0.6	2.5	14.0	1.2	3.4	0.1	0.4	0.0	0.1	0.0	0.0
Western Europe	57.2%	40.2	59.0	14.0	18.9	7.5	9.2	1.8	2.3	3.8	5.6	2.5	3.2	1.3	1.6	0.0	0.0	0.0	0.0
East Asia	30.8%	12.2	25.8	14.9	44.5	6.3	12.1	0.9	1.6	2.2	9.1	3.1	6.5	0.1	0.2	0.1	0.2	0.0	0.1
Central Asia	17.3%	13.5	54.2	1.6	12.0	0.6	2.4	0.0	0.2	2.4	30.3	0.2	0.8	0.0	0.0	0.0	0.1	0.0	0.0
Southeast Asia	21.7%	9.0	25.4	7.5	31.2	1.0	2.7	0.2	0.5	7.8	37.0	0.9	2.7	0.1	0.2	0.1	0.3	0.0	0.0
South Asia	8.7%	2.5	16.6	2.7	24.2	0.4	2.4	0.1	0.8	4.1	54.5	0.2	1.1	0.0	0.2	0.0	0.2	0.0	0.0
N. Africa, M. East	19.1%	9.4	35.7	5.1	26.2	1.8	6.4	0.1	0.3	5.2	28.5	0.7	2.4	0.0	0.2	0.0	0.2	0.0	0.1
Oceania	49.2%	30.7	46.6	19.8	25.9	10.1	12.7	3.2	4.2	3.0	5.3	3.5	4.3	0.7	0.9	0.1	0.2	0.0	0.0
Sub-Saharan Africa	19.7%	6.9	21.7	10.9	49.9	2.5	7.1	0.1	0.4	2.8	18.0	0.8	2.3	0.1	0.3	0.1	0.3	0.0	0.1

Figure 1. Scan results of IoT devices [1].

A large issue with IP cameras is unsecure default configurations using passwords easy to guess or crack [7]. Owners of these devices often don't bother changing these initial settings, allowing for greater-than-intended access to these cameras. Such camera feeds can be seen across the internet, such as Insecam, where thousands of unsecure camera feeds from across the world are publicly available [8].

Another method of security analysis is static analysis tools, such as Julia, ASTREE or GrammaTech CodeSonar. It has been noted that these static analysis tools can analyze 6 out of 10 OWASP Top 10 IoT Security vulnerabilities [9]. Both chosen devices do not include

generally easy access to their firmware, where the static analysis could be performed – this is left out of the scope.

Most of the consumer market IoT devices have not been analyzed in official reports or journals, but rather reviewed in tech magazines and websites. There is often no focus on the cyber security aspect, but rather the feature-set and price points. Such comparative reviews offer little to no insight to the security of the respective devices [10] [11].

3 Methodology

To analyze IoT devices security, similarly with any other devices, best practices, tools, and methods must be used. These include software and solutions best suited to simulate the perspective of a potential attacker, looking to exploit the device in question. The methods used to capture and analyze network traffic include port scanning, network traffic monitoring and web application vulnerability scanning.

3.1 Device choice

Two devices were chosen for the case study – the Xiaomi Mi Home 360 and Vimtag PTZ Cloud IP Camera.

The Xiaomi camera device was chosen due to the cheap price tag, globally known brand name and advertised functionality. This device was the Chinese brands first step into the consumer IoT camera market [10].

Supplied in the box are the following: charging cable (male USB to male micro-USB), a mount with screws (used to mount the camera on a wall or ceiling), warranty notice, user manual and the camera. Not supplied but externally added tools include a pin for resetting the device, a charging brick, and a microSD card.

The Vimtag camera device was chosen due to the cheap price point, being a less known brand, although still advertising a good scope of functionality. Connecting the Vimtag camera via network cable is a functionality, that the Xiaomi counterpart does not offer, but for conformity, the Vimtag is also set up and analyzed while using Wi-Fi. Supplied in the box are a charging brick and cable, a small ethernet cable, and a wall mount with screws.

These cameras are henceforth simply Xiaomi device and Vimtag device.

Also, for capturing and analyzing the network traffic, a personal laptop and home router will be used. A smartphone will be used for both devices' user interface management and operation.

3.2 Overview of Wireshark

An industry-standard tool for network traffic and packet analysis is Wireshark. Wireshark captures data from a network interface and breaks the capture down into frames, segments, and packets [12]. Wireshark will be used to capture communications from the devices, afterwards analyzing the contents. Like the case study at hand, Wireshark has been used for capturing and analyzing IoT device security before in similar security assessment settings [13].

3.3 Overview of Nmap

Nmap is a commonly used free-to-use and open-source utility for security auditing and network discovery. In the Windows suite it also includes an advanced graphical user interface named Zenmap and a few other tools [14]. It is a tool often used by security specialists or even malicious attackers when probing networks. Nmap will be used to gather data about the devices in question, providing data about open TCP and/or UDP ports and device information.

The two main profiles used for data gathering within the current scope are “Intensive scan” and “Slow comprehensive scan”. The latter provides a quick overview of TCP ports and found device information, while the former also includes UDP port scanning. This is much slower due to the nature of scanning TCP and UDP ports – the TCP ports respond with acknowledgements immediately, while the UDP traffic does not usually get a response. When Nmap is sending packets to UDP ports, open ports rarely reply to empty payloads, meaning that there is a state of open|filtered. This state cannot conclusively say whether the port is open or not, because if the port was closed, it might not always disregard the sent traffic and drop the packet similarly to if the port was open [15].

3.4 Overview of OWASP ZAP

OWASP ZAP is a free open-source penetration testing application, which is developed under the OWASP umbrella. The application works as a middle proxy between the web application and browser, intercepting and even modifying packets in between [16]. The application will

be used for penetration testing web applications present with the test case devices, where applicable.

3.5 Methods to gather internal network traffic

When looking at possible options to gather network data, that the devices receive and send, there are a few options to choose from:

- Monitoring wireless traffic with a network card (either separately connected to a device or integrated), that supports Monitor Mode in Wireshark.
- Setting up traffic capture on the router connected to the IoT Wi-Fi camera and dumping that traffic to a third device to then analyze it in Wireshark.
- Creating a Wi-Fi access point/hotspot with built-in Windows functionality, to which the devices can be connected to. This way the communications of the devices run through the access point device, where the traffic can be then monitored from Wireshark.

From the attacker's perspective, the most likely option would be to use the first option, as it requires less privileged access while still generating the same traffic, a possible scenario would be the following: an attacker with a mobile device, such as a laptop, gains access to a local Wi-Fi network, either bypassing the Wi-Fi security or just joining an unprotected network. Most likely, the attacker would have either a separate network card, which are readily available to purchase online, to connect to the laptop or have a network card integrated into the laptop, which supports wireless traffic Monitor Mode. The network is then monitored for traffic.

The second option could also be utilized by a potential attacker, but it requires further access and authorization. Access to the router might be more difficult to obtain, if the end goal is compromising only the IoT camera, although if the router is already accessible to the attacker, traffic from the devices can be monitored all the same.

The third option from an attacker's perspective is also quite possible to be used, by acting as a middleman between the router and camera. This is much harder to perform as a real attack because the middleman must be prepared during the device setup and this method is not usable after the device has already been set up.

If the given options are not viable, some network traffic should be visible from Wireshark when looking at the wireless traffic with promiscuous mode. This method is not viable for the full scope of traffic – besides communications from the host to router, only traffic/packets without recipients are visible from Wireshark.

3.6 Assessment creation methodology

The OWASP IoT 2018 list of vulnerabilities will be used for mapping found issues and vulnerabilities from the chosen devices. The 2018 version of the list is the latest, due to most vulnerabilities listed being connected to the main OWASP listings for web application vulnerabilities. Each point of the OWASP Top 10 IoT will be analyzed against the findings of testing and how applicable they are to the mentioned vulnerabilities. This will provide a good overview of the initial security of the devices, supplying a good baseline for an assessment.

4 Testing cases

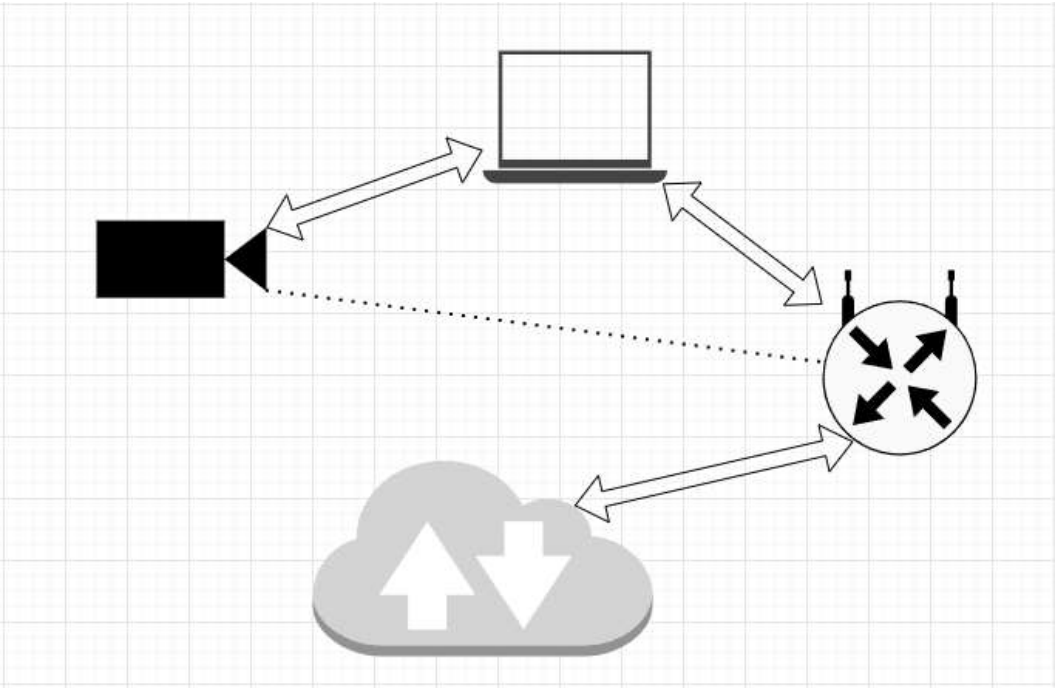

Figure 2. Network setup for experiments.

For data collection and further analysis, the network is set up as shown on Figure 2. In normal usage, the smart camera would connect directly to the router but for data collection purposes, a personal laptop has been set up as a middleman. This allows for packet traffic collection from the laptop. Such infrastructure may also emulate a possible Man-in-the-Middle attack from a threat actor. The laptop is connected to the router via Wi-Fi and using the Windows hotspot functionality, advertises a network connection, acting as an access point. IP addresses are not assigned to the cameras manually, DHCP is used instead. This exact setup can also be used as a threat actor, hoping to perform similar collection of data by getting the camera connection to their hotspot, which might be named similarly to the actual Wi-Fi network propagated nearby. Similar data collection can be done from the router itself, but the current setup was chosen for simplicity. This infrastructure is used for all experiments done with chosen case study devices, including Wireshark network traffic collection and Nmap port scanning.

4.1 Device setup and initial analysis

For the Xiaomi device, setting the camera up starts by connecting the charging cable, after which the device will await instructions. A smart device such as a personal smartphone is needed to install the Xiaomi Home app, which handles most of the setting up. The first connection is made by proximity between the smart device and camera, connection to the local network is followed by that. If the wrong network credentials are entered, the device will announce it. At one point of the setup, the personal smart device creates a local Wi-Fi hotspot for the camera to connect to. Further authentication is made by scanning the QR code underneath the device. After the mentioned steps, the Xiaomi device is operational.

Setting up the Vimtag device is quite similar in its process to the Xiaomi device, although further authentication is required to be performed. During the process of setting up, sound signals from the Vimtag device and smart device, used for setting up, link up to each other. Another difference is the connection to the local network – the Vimtag device seems to hop over the setup device and concludes the connection, while the Xiaomi user interface within the setup device creates a temporary hotspot to which the Xiaomi device first connects to, before establishing a direct connection to the access point.

Initial hardware analysis concludes that both devices are external power dependent, meaning that there is no batteries or onboard power storage. This impacts the availability of the devices heavily, as they provide security if there is power. The vulnerability can be mitigated with the use of a UPS device in case of power outages, but still leaves the devices vulnerable to a possible threat agent simply unplugging the power cords. Both devices also include physical reset buttons, used to factory wipe the devices. The Vimtag device has the reset button on the back of the device in an accessible spot. The Xiaomi devices reset button on the other hand is visible only when the camera is pointing upwards and requires a pinhole tool to reset it.

Setting up the laptop for packet capture consists of advertising a Wi-Fi network via hotspot, connecting the devices to the network and starting to capture packets. After device setup, these packets are immediately visible in Wireshark.

The major difference in setting up the two devices was an added setup feature for the Vimtag device, which synchronizes and authenticates the camera device with the smart device used for

setting up using sound signals in proximity. The difference can also be seen in Wireshark, as the advertised and used network only gets connected to the Vimtag after setup, while the Xiaomi device starts producing traffic during the setup process.

Multiple .pcap capture files of device setup were saved for further analysis from Wireshark. These captures were collected during initial device setups for both devices.

4.2 Experiments

To further understand and analyze the security of the chosen devices, best practice tools and methods must be used. Experiments such as Nmap port scanning and Wireshark traffic capture allow for data collection within the home network scope, which can then be analyzed further and mapped to the OWASP Top 10 IoT list of vulnerabilities to create a thorough security assessment.

4.2.1 Differentiate between traffic

Once the Xiaomi device is turned on, a new entry in the router table is created. The default name of the device “chuangmi_camera_026c02” quickly reveals the IP and MAC address of the device. A similar entry is created for the Vimtag device once it has been set up.

After initial device setup, both devices are connected to the propagated hotspot. To differentiate between traffic, it is necessary to know what IP addresses the devices are assigned by DHCP to then filter out only the traffic generated by one device within Wireshark. These IP addresses are shown within the hotspot tool in Windows, which displays all connected devices to the access point. If the names of the devices do not hint at the device itself, the names could be correlated with the moment of connection once the connection table has an addition.

4.2.2 Grouping of packets, analysis

To understand exactly what to look for when analyzing the traffic generated, some test cases can be used and captured. These would include traffic, that is generated when:

- connecting to the device,

- moving the camera,
- making a screenshot,
- capturing a video,
- sending and receiving voice communications, or
- setting up the device.

Most likely the captured network traffic during each test will yield similar results, meaning that the type of encryption or communication protocol will not differ from test to test. Still, it is best to run through each test individually to confirm the similarities.

Initial attempted method of reconnaissance was using the method of listening for packets from a personal laptop while in promiscuous mode in Wireshark. The devices are turned on and operational. As a test case, multiple operations are run on the devices through using their respective user interfaces from the personal smart device authenticated with the cameras. With all these operations, Wireshark does not capture any packets from the respective devices. Also, turning the devices off and on did not reveal any handshakes. This testing does not provide any usable information to a potential attacker – an increased access to the router or Man-in-the-Middle attack must be performed to gather further data.

4.2.3 Wireshark capture analysis

Upon initial inspection of the Wireshark captures, the first big difference is noticeable in the device communication – the Xiaomi device sends predominantly UDP packets to the UI, while the Vimtag also sends TCP packets. The Vimtag device sends camera feed in UDP packets as well.

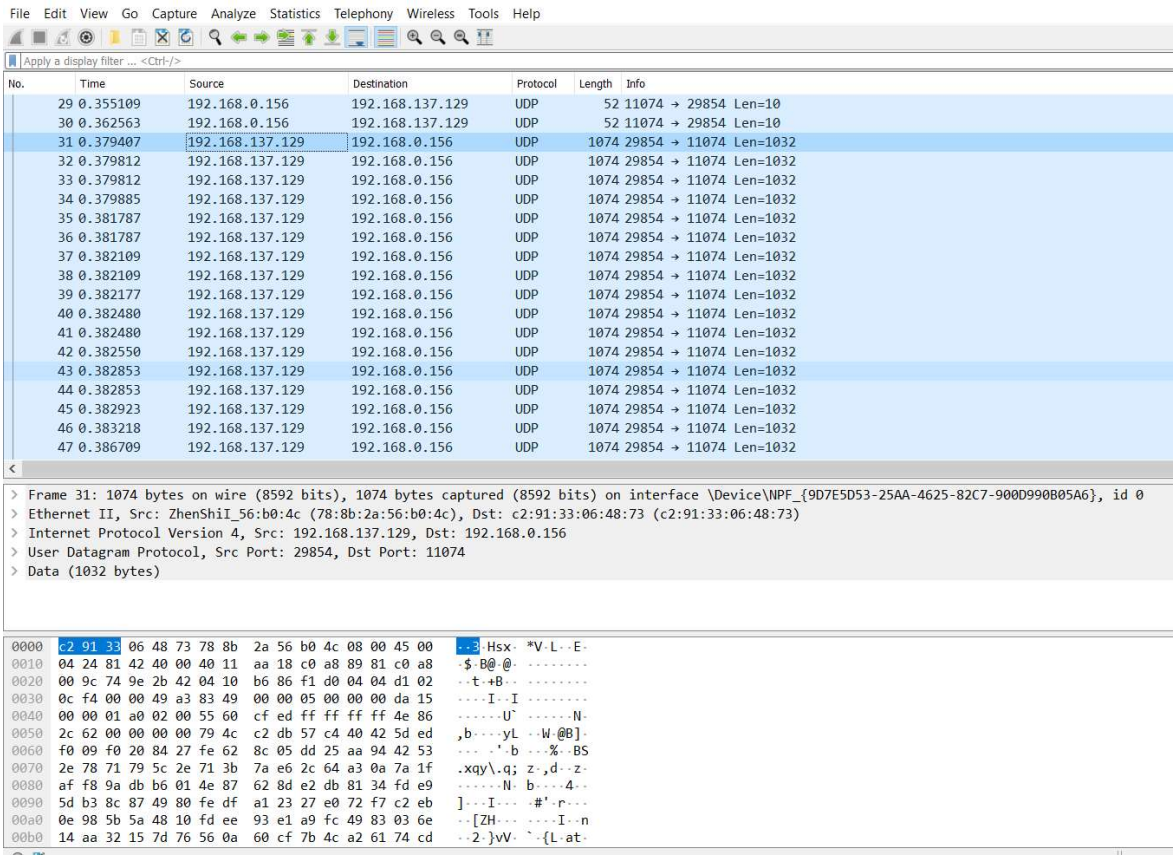

Figure 3. Wireshark capture example.

In Figure 3, an example of a UDP stream originating from the Xiaomi device can be seen. The UDP packets do not contain information about the communication type and Wireshark does not recognize any RTP stream, if attempted to decode as such. With these raw packets, it is also unlikely to understand the method of encryption or communication without another avenue into the device firmware, examining the methods from within. These gathered examples do not provide great insight nor do they show any blatant vunlerabilities.

4.2.4 Nmap scan, open services

Nmap was used to scan the device for any open ports, initially running a “Intense scan” profile – no open ports were found for the Xiaomi device and not a lot of device information, while the Vimtag device exposed an open TCP port, also exposing with 95% certainty the operating system of the device, which Nmap believes to be Linux 3.1. This information is presented in Figure 4.

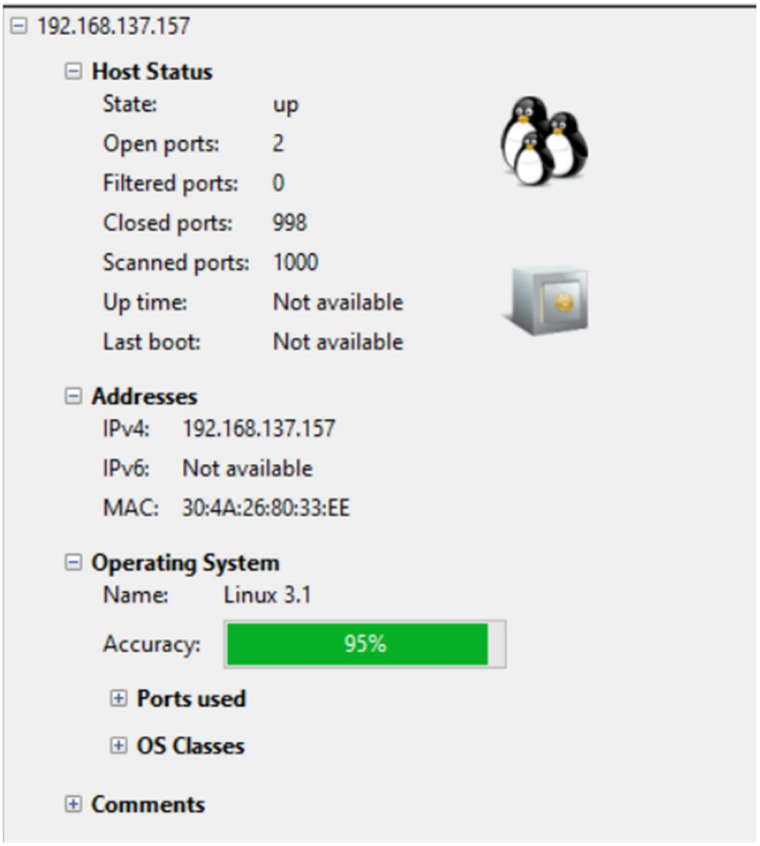

Figure 4. Nmap results of Vimtag device, information presented.

A quick MAC address lookup provides additional information about the device manufacturer, which specializes in IoT devices, as shown in Figure 5.

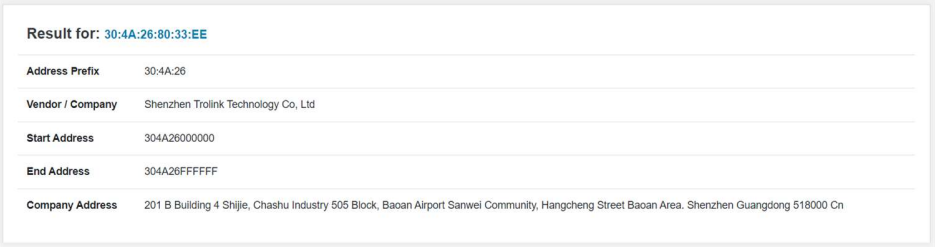

Figure 5. MAC address lookup showing information about device manufacturer.

It is also possible to connect to the device through an HTTP web user interface, which will be further analysed.

Afterwards, a “Slow comprehensive” scan profile was also completed, resulting in 13 open|filtered UDP ports found for the Xiaomi device, three of which are running on ports believed to be the services: cplscrambler-al, radacct and bo2k. Upon a second comprehensive

scan, 19 open|filtered UDP ports are shown. After completing the same slow scan for the Vimtag device, also 13 open|filtered UDP ports were discovered, of which two services are believed to be ftps-data and adobeserver-3. The results of the “Slow comprehensive” scan are shown in Figure 6.

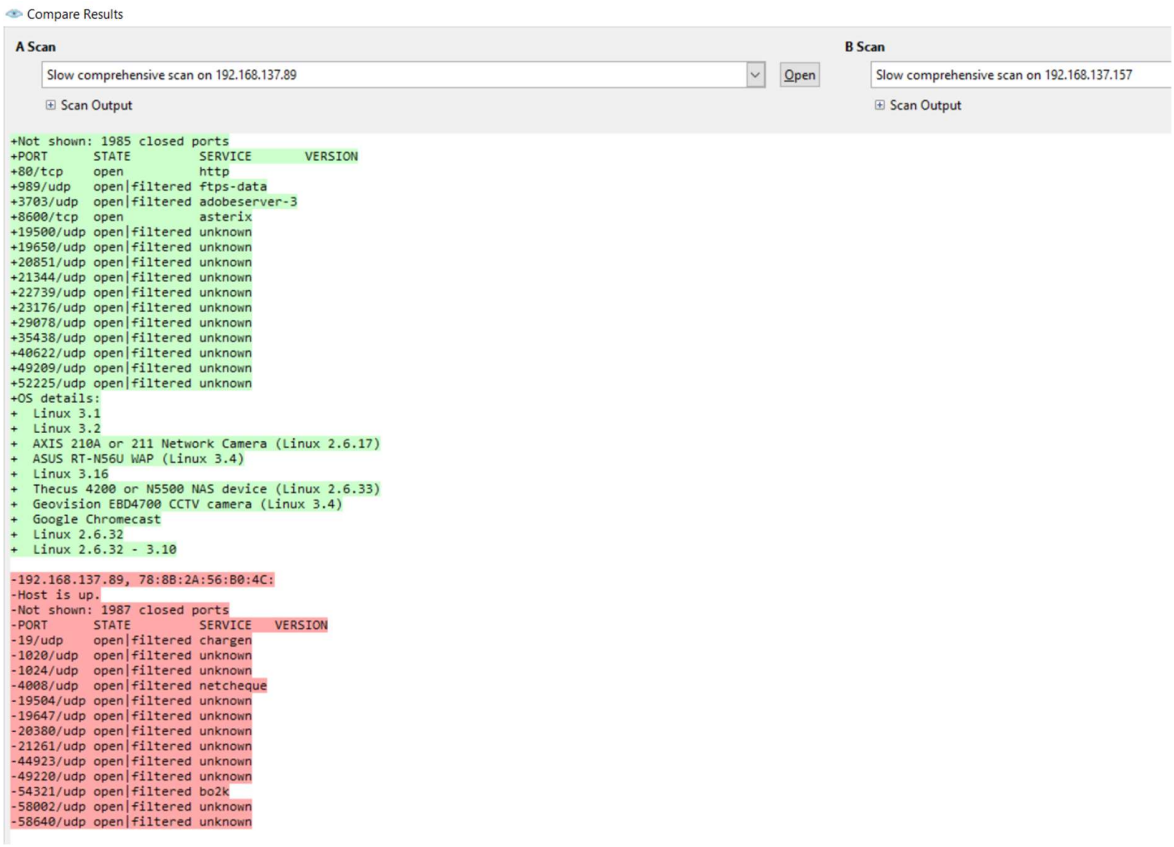

Figure 6. Slow scan results showing many open|filtered UDP ports for the Xiaomi device.

As a disclaimer, these found services are most likely false positives, due to the nature of UDP port scanning. When scanning for open UDP ports, the scanner believes the port to be open, if no response is given and guesses the running service based on the port used by default [15].

Nmap found bo2k, also known as Back Orifice 2000 service running on UDP port 54321. Bo2k is an old trojan backdoor remote-control application originating from around 1999 [17]. The other services mentioned also seem unrelated to the device operations, meaning most likely these are not the services running on these ports.

4.3 Analysis of web interface, OWASP ZAP

The port scanning done previously shows an open TCP port, which may allow access to the Vimtag device. This is verified by opening the device IP from the web browser, which opens a web interface with login options. The OWASP ZAP tool is then used to automatically scan for vulnerabilities of the web interface, the results of which are shown in Figure 7.

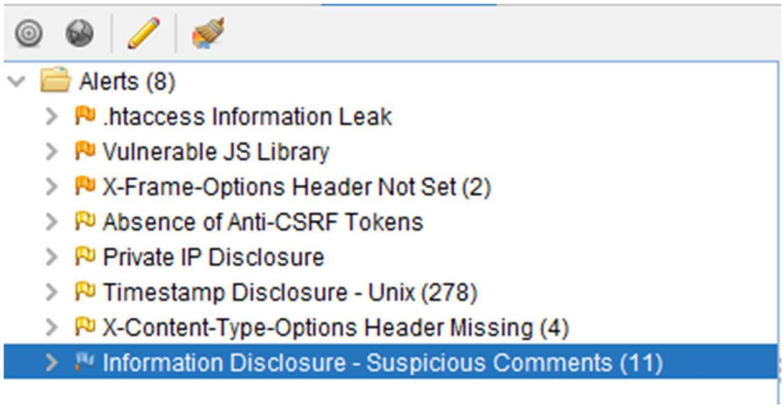

Figure 7. Results of OWASP ZAP automated scan against the web application of the Vimtag device.

These results offer an insight into some aspects of the web application security.

The first alert raised mentions .htaccess Information Leak, which can allow an attacker to alter the configuration of the web server, enabling or disabling additional functionalities. The second alert is about a vulnerable JavaScript library used in the web application, which could be exploited. The absence of Anti-CSRF tokens means that the web application could be vulnerable to cross-site request forgery. CSRF attacks work in cases, where the victim has an active session with the web application, or the victim is authenticated using HTTP auth [18].

The vulnerable JavaScript library is an outdated version of Jquery, which is shown on Figure 8. There are 7 known vulnerabilities known for Jquery 1.8.3, including Cross-Site Scripting, Arbitrary Code Injection and Prototype Pollution [19].

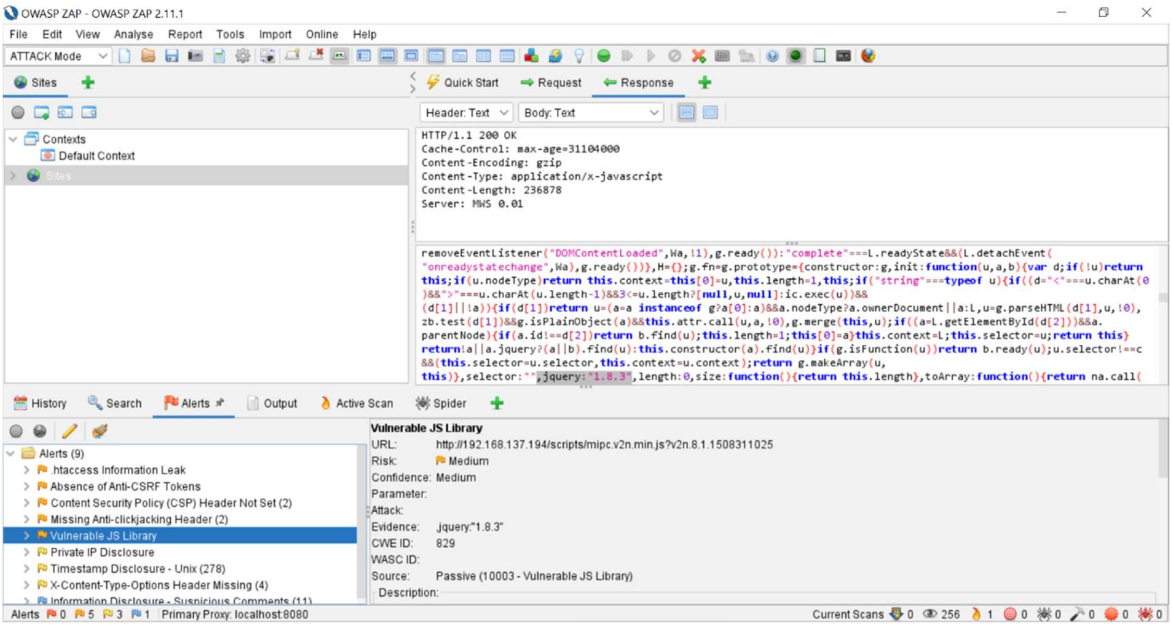

Figure 8. Vulnerable version of Jquery used in the web application of the Vimtag device.

The web application was further analysed with OWASP ZAP, where the HTTP payload of the website was checked for any plaintext credentials, that could possibly be captured. Figure 9 shows the HTTP request, where only the username exists as plaintext, which does not impact security, because the username is hardcoded into the login form by the device. The password is obfuscated with an unknown method.

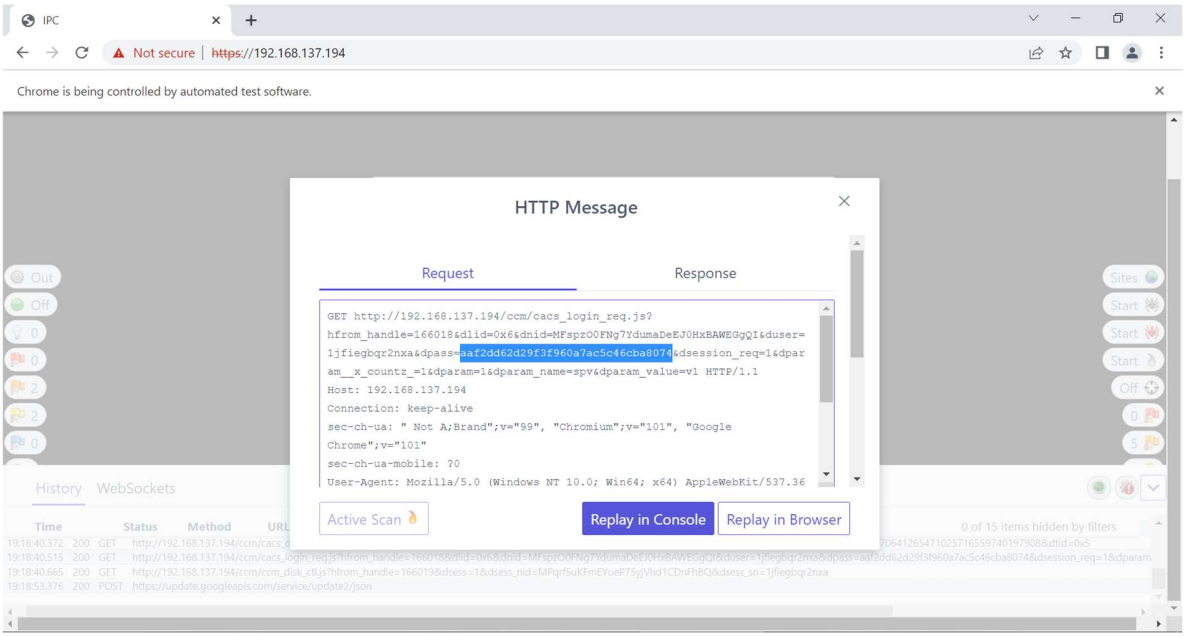

Figure 9. Intercepted HTTP payload.

4.4 Analysis of external threats outside of home network

After setting the Xiaomi device up, if turned on, will be visible in the Mi Home app. This application relied on authentication methods of the smart device, meaning it did not reauthenticate the application user once the app had been launched. If the smart device linked with the camera did not sufficiently authenticate the user or did not have any authentication method set up whatsoever, it critically exposed privacy – if an attacker were to find or steal this device, they would have had the same controls over the smart device as the proper user. Essentially the smart device attempted to guarantee the safety and privacy of user info up until it reached the device, from there it gave the reigns of safety to the user. Since a software update for the Mi Home application, it now prompts to set up a password for the camera, although this can be dismissed by the user and is not required.

The Vimtag user application does prompt the user to set up a password for the camera quite largely, without the ability to ignore the message during regular usage. This message can still

be disregarded and the Vimtag device does remain operable, but the quality of usage will be diminished.

Depending on the install location, the devices also have physical controls, which can be abused by a potential threat actor to either turn off or alter the device operations. For the Xiaomi device, resetting the device with physical controls does need a tool (a small pinhead, same tool used for removing the SIM tray of modern smartphones), which the Vimtag does not.

5 Security analysis results mapped to OWASP

The last OWASP IoT Top 10 was compiled in 2018 [7] and includes:

- I1 Weak Guessable, or Hardcoded Passwords
- I2 Insecure Network Services
- I3 Insecure Ecosystem Interfaces
- I4 Lack of Secure Update Mechanism
- I5 Use of Insecure or Outdated Components
- I6 Insufficient Privacy Protection
- I7 Insecure Data Transfer and Storage
- I8 Lack of Device Management
- I9 Insecure Default Settings
- I10 Lack of Physical Hardening

5.1 Weak Guessable, or Hardcoded Passwords

Neither of the devices come with previously set up hardcoded/unchangeable passwords.

5.2 Insecure Network Services

No unnecessary and insecure services were found to be exposed by either device. The Xiaomi device did not propagate any open TCP ports running known services and the results of the UDP scans were inconclusive. The ports found were most likely custom chosen.

5.3 Insecure Ecosystem Interfaces

Both the Vimtag and Xiaomi devices suggest adding a password within the user interface after setting them up. Both devices also allow you to operate the devices without setting a password, which in turn means the user interface security is only behind the smart device authentication.

Because the application does not check for authentication complexity on the smart device, it means it allows operation on very insecure settings.

The web application included for the Vimtag device also shows multiple alerts from vulnerability scanning, which are shown in Figure 7 – this suggests risks regarding insecure web application.

5.4 Lack of Secure Update Mechanism

As both devices constrict administrative access to firmware, it is unclear whether the update mechanism is secured.

5.5 Use of Insecure or Outdated Components

The Vimtag web application was found to be using a vulnerable version of the Jquery JavaScript library, which poses a great risk. No similar evidence is found from the Xiaomi device. Regarding firmware or operating system components, they remain outside of the scope.

5.6 Insufficient Privacy Protection

Specific privacy protection mechanisms are not within the current scope, which means no indications tested and found. An example of insufficient privacy protection would include improper collection and storage of personal user information in the devices' ecosystems, which cannot be tested in the current scope.

5.7 Insecure Data Transfer and Storage

While data in transfer within the home network is properly encrypted, both devices have easily accessible microSD slots where data at rest is quite vulnerable to physical accessing. This rather poses a risk, if the medium is used – the microSD slot does not have to be used for local data storage within the device. If used, a malicious threat actor may gain physical access and access the data. The vulnerability could also be accounted for under lack of physical hardening.

5.8 Lack of Device Management

Because both devices are aimed at the consumer market, they lack advanced administrative capabilities, such as administrator defined gateways for connections, further capabilities for disconnecting from the proposed cloud solution offered by the manufacturers, custom defined encryption methods, custom chosen ports and more. Similar options are quite likely to be included for devices aimed at enterprise markets.

5.9 Insecure Default Settings

Default settings are perhaps not fully applicable in this scope, because most default settings are applied either in the factory or exist solely in the ecosystem interfaces of the devices.

5.10 Lack of Physical Hardening

Both devices operate on wall power without backup batteries, which makes them dependent on power delivery. In case of power failure or simply unplugging the devices from the wall takes the devices offline, severely impacting availability. In terms of physical access to reset the devices, the Xiaomi reset button is somewhat hidden and requires an extra tool to be used, while the Vimtag device has an exposed reset button in plain view, which can be used by a malicious threat actor to simply reset the device to factory settings.

The mapped findings support results of evidence of insecure practices with both the Xiaomi and Vimtag devices. Both devices show weakness in similar aspects, with the larger difference being the web application hosted on the Vimtag device, which upon vulnerability scanning shows evidence of insecurity. A similar web application does not exist on the Xiaomi device, which concludes a reduced attack surface. Besides the web application, both devices operate on a cloud solution user interface on smart devices – downloadable applications from respectable app stores. Both these user interfaces work quite similarly in terms of capabilities and security. Both devices also lack administrative capabilities, with reduced access to firmware and operational services and systems.

6 Conclusions

A better overview of security for the test case devices has been achieved through scanning for vulnerabilities and assessing security properties. The authors research exposes multiple potential gaps in the security of the devices, pertaining specifically to points of insecure ecosystems, lack of physical hardening of the devices and insecure data transfer and storage. Both devices lack physical hardening due to no onboard backup power, meaning that they are power dependent. At the same time, both devices have onboard microSD storage, which is easily accessible for a potential threat actor. The Vimtag device also hosts a web application, the automatic scanning from OWASP ZAP shows multiple possible vulnerabilities, that could potentially be exploited.

Potential future research would include increasing the scope of research for these same smart devices, including greater firmware and mobile application vulnerability scanning and analysis. This would increase the comprehensibility of security of these devices.

References

[1] D. Kumar, K. Shen, B. Case, D. Garg, G. Alperovich, D. Kuznetsov, R. Gupta and Z. Durumeric, "All Things Considered: An Analysis of IoT Devices on Home Networks," 14-16 August 2019. [Online]. Available: https://www.usenix.org/system/files/sec19-kumar-deepak_0.pdf. [Accessed 12 November 2021].

[2] M. De Donno, N. Dragoni, A. Giaretta and A. Spognardi, "DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation," *Security and Communication Networks,* vol. I, no. 1, pp. 1-2, 2018.

[3] Telecommunication Standardization Sector of ITU, "Overview of the Internet of Things," International Telecommunication Union, Geneva, 2012.

[4] T. Alladi, V. Chamola, B. Sikdar and K.-K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," *IEEE Consumer Electronics Magazine,* vol. 9, no. 2, p. 6, 2019.

[5] S. Floderus and V. Tewolde, "Analysing privacy concerns in smart cameras," Bleking Institute of Technology, Karlskrona, 2021.

[6] P. Vennam, P. T. C, T. B. M, Y.-G. Kim and P. K. B. N, "Attacks and Preventive Measures on Video Surveillance Systems: A Review," *DOAJ Directory of Open Access Journals,* vol. 11, no. 12, p. 4, 2021.

[7] "OWASP Internet of Things Project," OWASP, 1 November 2019. [Online]. Available: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10. [Accessed 13 November 2021].

[8] F. Ahlgren, "IoT Camera Security Case: Hikvision and Label X cameras," Turku University of Applied Sciences, Turku, 2020.

[9] P. Ferrara, A. K. Mandal, A. Cortesi and F. Spoto, "Static analysis for discovering IoT vulnerabilities," *International Journal on Software Tools for Technology Transfer,* vol. 23, no. SPIoT 2019, pp. 71-88, 2021.

[10] A. Sharma, "Xiaomi Mi Home Security Camera Basic VS Mi Home Security Camera 360 Degrees; Comparing the two smart home surveillance cameras from Xiaomi," 10 Aprl 2019. [Online]. Available: https://www.digit.in/features/internet-of-things/mi-home-security-camera-basic-vs-mi-home-security-camera-360-degree-comparing-the-two-smart-home-sur-47409.html. [Accessed 13 March 2022].

[11] H. Jonnalagadda, "Xiaomi Mi Home Security Camera 360 review: An affordable home monitoring solution," 27 September 2018. [Online]. Available: https://www.androidcentral.com/xiaomi-mi-home-security-camera-360-review. [Accessed 13 March 2022].

[12] J. Bullock, J. T. Parker, A. Gordon and J. T. Parker, "What Is Wireshark?," in *Wireshark for Security Professionals : Using Wireshark and the Metasploit Framework*, John Wiley & Sons, Incorporated, 2017, p. 2.

[13] M. Chernyshev and P. Hannay, "Security Assessment of IoT Devices: the Case of Two Smart TVs," in *13th Australian Digital Forensics*, Perth, 2015.

[14] "Nmap.org," [Online]. Available: https://nmap.org/. [Accessed 14 November 2021].

[15] "Nmap Network Scanning UDP Scan," [Online]. Available: https://nmap.org/book/scan-methods-udp-scan.html. [Accessed 14 November 2021].

[16] ZAP Dev Team, "Getting Started," OWASP ZAP, [Online]. Available: https://www.zaproxy.org/getting-started/. [Accessed 3 May 2022].

[17] R. Ferrill, "Back Orifice 2000 (BO2K) – The Insider Threat," *GIAC Practical Repository,* no. 2.1a, p. 3, 2003.

[18] ZAP Dev Team, "ZAP Alert Details," OWASP, [Online]. Available: https://www.zaproxy.org/docs/alerts/. [Accessed 3 May 2022].

[19] Snyk.io, "jquery@1.8.3 Vulnerabilities," Snyk, [Online]. Available: https://snyk.io/test/npm/jquery/1.8.3. [Accessed 12 May 2022].

Appendix 1 – Non-exclusive license for reproduction and publication of a graduation thesis[1]

I Oliver Erlich

1. Grant Tallinn University of Technology free license (non-exclusive license) for my thesis “Consumer Grade IoT Security Analysis: a Case Study”, supervised by Mohammad Tariq Meeran
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive license.
3. I confirm that granting the non-exclusive license does not infringe other persons’ intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

16.05.2022

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.