



Analysing privacy concerns in smart cameras

in correlation with GDPR and Privacy by Design

Sebastian Floderus

Vincent Tewolde

This thesis is submitted to the Faculty of Computing at Blekinge Institute of Technology in partial fulfilment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

The authors declare that they are the sole authors of this thesis and that they have not used any sources other than those listed in the bibliography and identified as references. They further declare that they have not submitted this thesis at any other institution to obtain a degree.

Contact Information:

Author(s):

Sebastian Floderus

E-mail: sefl16@student.bth.se

Vincent Tewolde

E-mail: vite16@student.bth.se

University advisor:

Docent Emiliano Casalicchio

Department of Computer science

Faculty of Computing
Blekinge Institute of Technology
SE-371 79 Karlskrona, Sweden

Internet : www.bth.se
Phone : +46 455 38 50 00
Fax : +46 455 38 50 57

Abstract

Background. The right to privacy is every persons right, data regulation laws such as the GDPR and privacy preserving concepts like Privacy by Design (PbD) aid in this matter. IoT devices are highly vulnerable to attacks because of their limited storage and processing capabilities, even more so for internet connected cameras. With the use of security auditing techniques and privacy analysis methods it is possible to identify security and privacy issues for Internet of Things (IoT) devices.

Objectives. The research aims to evaluate three selected IoT cameras' ability to protect privacy of their consumers. As well as investigating the role GDPR and PbD has in the design and operation of each device.

Methods. A literature review was performed in order to gain valuable knowledge of how to design a case study that would evaluate privacy issues of IoT devices in correlation with GDPR and PbD. The case study consists of 14 cases designed to explore security and privacy related issues. They were executed in a monitored and controlled network environment to detect data flow between devices.

Results. There was a noticeable difference in the security and privacy enhancing technologies used between some manufactures. Furthermore, there was a distinct disparity of how transparent each system was with the processed data, which is a crucial part of both GDPR and PbD.

Conclusions. All three companies had taken GDPR and PbD into consideration in the design on the IoT systems, however to different extents. One of the IoT manufactures could benefit from incorporating PbD more thoroughly into the design and operation of their product. Also the GDPR could benefit from having references to security standards and frameworks in order simplify the process for companies to secure their systems.

Keywords: Privacy by Design, GDPR, IoT, security, data management

Acknowledgments

We would like to thank Emiliano Casalicchio, our supervisor at BTH, for guiding us throughout the study and instructing us how to arrange the thesis. Emiliano also assisted us with deciding a topic and research questions.

We would also like to thank Thomas Edhoff, our supervisor at Knowit. We have received extremely valuable support for all matter regarding the case study and technologies. Thomas was also involved in the topic selection.

Contents

Abstract	i
Acknowledgments	iii
1 Introduction	5
1.1 Problem statement	6
1.2 Aim and objectives	6
1.3 Research questions	7
1.4 Scope and limitations	7
1.5 Ethical consideration	7
1.6 Document outline	8
2 Background	9
2.1 Privacy	9
2.1.1 Definition	9
2.1.2 Legislation & GDPR	9
2.1.3 Privacy by Design	11
2.2 Internet of Things systems	12
2.2.1 Smart cameras	12
2.3 Security auditing and privacy analysis	13
2.3.1 Reconnaissance	13
2.3.2 Network communication	14
2.3.3 Android application	14
2.3.4 Privacy analysis	14
2.4 Certificate Authority	15
3 Related works	17
4 Method	19
4.1 Research method	19
4.2 Literature review	19
4.2.1 Databases and keywords	19
4.2.2 Selection criteria	20
4.3 Privacy by Design and IoT device selection	21
4.3.1 Selection of principles in Privacy by Design	21
4.3.2 Selection of IoT devices	21
4.4 Case study	22
4.4.1 Environment setup	22

4.4.2	Tools and techniques	25
4.4.3	Case studies	27
4.4.4	Privacy notices and consent forms	34
5	Results	37
5.1	Literature review results	37
5.2	Summary of security assessment	39
5.2.1	Arlo	39
5.2.2	Ring	39
5.2.3	Foscam	39
5.3	Case studies result	40
5.3.1	Case study I	40
5.3.2	Case study II	40
5.3.3	Case study III	41
5.3.4	Case study IV	42
5.3.5	Case study V	42
5.3.6	Case study VI	43
5.3.7	Case study VII	44
5.3.8	Case study VIII	44
5.3.9	Case study IX	44
5.3.10	Case study X	44
5.3.11	Case study XI	45
5.3.12	Case study XII	45
5.3.13	Case study XIII	46
5.3.14	Case study XIV	47
5.3.15	Privacy notice questions result	49
6	Analysis and Discussion	55
6.1	Research limitations	55
6.2	Case study analysis and discussion	56
6.2.1	Case study I	56
6.2.2	Case study II & III	56
6.2.3	Case study IV	56
6.2.4	Case study V	57
6.2.5	Case study VI	57
6.2.6	Case study VII	58
6.2.7	Case study VIII	58
6.2.8	Case study IX	58
6.2.9	Case study X	58
6.2.10	Case study XI	59
6.2.11	Case study XII	59
6.2.12	Case study XIII	59
6.2.13	Case study XIV	60
6.2.14	Privacy notice analysis	61
6.3	Discussion of case study and findings	61
6.3.1	Research Question 1	62
6.3.2	Research Question 2	63

6.3.3	Research Question 3	63
7	Conclusions and Future Work	65
7.1	Future work	66
A	IP geo location	73
B	Android application permissions	77

List of Figures

4.1	Environment Setup	23
5.1	Wireshark conversations	41
5.2	Foscam: RTSP authentication method	42
5.3	Foscam: Encrypted traffic shown in cleartext	43
5.4	Foscam: Unknown CA response	43
5.5	Arlo: Encryption and encoding classes	45
5.6	Command for identifying RSA strings	45
5.7	Foscam: Non-trusted encryption packages	45
5.8	Ring Always Home: Offers the user ability to alter privacy settings .	46
A.1	Arlo: Geo location for IP addresses communicating with device . . .	73
A.2	Foscam: Geo location for IP addresses communicating with device . .	74
A.3	Ring: Geo location for IP addresses communicating with device . . .	75
A.4	Ring: Geo location for IP addresses communicating with device, part 2	76
B.1	Arlo android application permissions	78
B.2	Ring android application permissions	79
B.3	Foscam android application permissions	80

List of Tables

4.1	List of keywords	20
4.2	Environment details.	24
4.3	Arlo specifications	25
4.4	Ring specifications	25
4.5	Foscam specifications	25
4.6	Test description overview	28
4.7	Privacy notice information	35
5.1	Papers based on RQs	37
5.2	Researched literature overview	38
5.3	DNS request made by devices	40
5.4	Foscam: Running services on the camera device	42
5.5	Identifiable data from the taint analysis	47
5.6	Summarised result of reviewing the Privacay notice	50

In recent years *Internet of Things* (IoT) devices have grown at a tremendous speed. There are roughly 21.7 billion connected devices worldwide, at the end of 2020 it was predicted that 11.7 billion of those devices would be IoT devices. Different sources anticipate different numbers, however by 2025 it is predicted that the number of IoT devices will grow to somewhere between 24-30 billions [1, 2]. IoT devices can be useful in many different areas such as smart homes, healthcare, transport and others. Example of devices are smart cameras, smart locks, thermostats, cars connected to the internet and more. However many IoT device manufacturers neglect proper security implementations such as, security testing, encryption, certification and patching of new vulnerabilities [3]. Since IoT devices are well known for having poor security standards, it is an attractive target for attackers. In 2016 the newly unique Mirai botnet emerged, it was unique because it had gained control over 24.000 IoT devices with a large chunk of devices being cameras connected over the internet. It managed to disrupt large parts of the internet by Distributed Denial of Service (DDoS) attacks, among other Liberia's entire internet connection and a German internet service provider (ISP) [4]. From the emergence of the Mirai botnet came many other variants, one of them being the Torii botnet. Which instead of performing DDoS attacks had the goal to exfiltrate sensitive information from the IoT devices [5]. A research conducted by the SAM Seamless Network's Threat Lab, concluded that IoT smart cameras are the most vulnerable systems within smart homes, 47% of all hacking attempts targeted these devices [6].

The *General Data Protection Regulation* (GDPR) is a law passed by the European Union that came into effect in May, 2018. The regulation target organisations that collect and handle data of people living in the EU. The intention of GDPR is to protect the privacy of individuals, if an organisation violates the privacy and security standards they could suffer heavy fines . [7]

The concept of *Privacy by Design* (PbD) is to embed privacy measures and privacy-enhancing technologies into the design of software and the system has been around since the 1990's. PbD consists of seven foundational principles that serve as guidelines when designing systems that manages personal information, the goal is to ensure privacy and maintaining control over user's data

The aim of this research is to study the privacy concerns regarding IoT cameras, what kind of data is stored and how is it managed? In addition, explore how data regulation laws such as GDPR impacts IoT device design and operation, as well as look into how well the PbD principles are used in the IoT system and what can be improved.

1.1 Problem statement

Some published articles have examined the privacy and security issues regarding IoT cameras [8–11]. However in most cases, IoT security research often has narrow methodologies for security auditing or selection of devices. There are also studies exploring privacy issues challenges in IoT systems in correlations with GDPR and PbD [12–14]. Although these papers deliver insightful information and conclusions, they are often based on theoretical knowledge and not practical tests. Therefore they do not demonstrate real world examples of how data actually is processed within an IoT system. Since GDPR is a quite newly implemented regulation and the area of IoT systems can be so wide and diverse. There is a somewhat lack of research that investigate the connection between data regulation laws and real world IoT systems, even more so regarding IoT smart cameras. Since IoT systems often have limited storage and processing capacity, security measures are oftentimes neglected. GDPR and PbD can therefore be a useful tool to improve the security and privacy related issues in IoT systems, however it is unclear to what extent different IoT manufacturers takes GDPR and PbD in to consideration.

1.2 Aim and objectives

This project focuses on researching IoT cameras' data management to see if GDPR conditions are met. By examining the cameras data's lifecycle, the goal is to discover how well the data is protected and what mitigation is implemented to respect the privacy of the user. The gathered outcome will be compared to best practices of the PbD that ensures GDPR compliance. Because GDPR currently does not propose one standard framework for IoT privacy concerns to adhere to, the risk for poor security implementation increases regarding users' integrity. This indicates that there could be several IoT cameras on the market not enforced with the proper privacy protection. In this project, physical and technical tests on three selected IoT devices will investigate whether or not PbD has been taken in to consideration when designing the IoT camera system.

Objectives

1. Research related work and review GDPR regulations related to the PbD principles selected
2. Explore mitigation techniques that ensures users' privacy in selected IoT cameras
3. Observe the camera's data management by penetration testing
4. Compare results from previous step to examine how it complies with the PbD principles
5. Evaluate each device's characteristics and potentially recommend improvements

1.3 Research questions

IoT devices often lack the computing power and memory capability compared to computers and servers, therefore, the general security is reduced. Combining this with the absence of official frameworks to protect user privacy, these devices become desirable targets for cyber-attacks which could lead to serious consequences for user confidentiality and integrity.

- RQ 1: What type of data is stored on the selected IoT smart cameras, how is the data managed and what countermeasures are implemented to protect the privacy of the user?
- RQ 2: to what extent are the Privacy by Design principles applied to application and design? What can be improved?
- RQ 3: How does the current data regulation laws (GDPR) impact or should impact IoT device design and operation?

The first research questions aims to answer what general information is saved in the selected cameras and clarify what methods are put in by the manufacturers to achieve privacy for the users.

RQ 2, focuses on how the three selected PbD principles are met in the embedded application and device design of the chosen IoT cameras. Also, to explore possible improvements for either the embedded application or device design to meet the PbD requirements.

RQ 3, examines how the current GDPR law affects the design and operation in IoT cameras. What possible modifications are necessary for current IoT cameras in order to attain GDPR compliance.

1.4 Scope and limitations

The scope of this research is limited to testing three IoT camera devices: Ring camera, Arlo essential camera and Foscam C2M camera. Initially different areas of IoT devices were investigated by reading similar studies and evaluating privacy issues in IoT, among other medical IoT and wearable IoT [15, 16]. However these devices are in many cases expensive or difficult to acquire physically. Therefore, IoT cameras were selected since they are easier to come by and more affordable, as well as being a popular target of attackers. Furthermore the focus of the security auditing is foremost based on the network-side and android application, meanwhile the firmware is considered to be out-of-scope of this thesis.

1.5 Ethical consideration

The case study is executed in a controlled environment with never before used IoT devices, so there is no sensitive data from previous users. Instead random generated Personal Identifiable Information (PII) is used with intention of simulating real

camera usage. The study is completed on real consumer available IoT devices, therefore the case studies are designed to only assess the local soft- and hardware of the systems. Traffic between devices and cloud services will only be observed and not tampered with to avoid interference and in respect to legalisation. Neither is any code altered when reviewing the android source code.

When or if a critical vulnerability is found the company is contacted in a responsible fashion, describing the process of finding the weakness and how to potentially fix the issue. This is performed before any publications are officially made, which gives the company a reasonable time frame to fix the issue.

1.6 Document outline

Background describes information necessary to understand the content of the thesis. It explains the basics of the privacy legislation GDPR and the PbD framework for IoT devices. It provides fundamental knowledge about the technical aspects like IoT, smart cameras and certificate authority.

Related works informs of relevant papers that research closely connected topics with this thesis work, which gives guidelines of how to form the test design.

Method defines the research method, literature review, the case study setup and all case studies together with description with its purpose. It describes the selection of PbD principles, IoT cameras and what tools and techniques were practised to execute the tests.

Results present literature review conclusion and the outcome of the case studies in a categorised and systematic approach.

Analysis and Discussion highlights the interesting and valuable findings of the case study and privacy notice analysis. It discusses the findings and answers the research questions based on the information gathered.

Conclusion and Future work summarises the thesis total outcome and suggests relevant research topics for future studies.

The background chapter discusses information that is necessary for the reader to grasp the content of this project to a greater extent.

2.1 Privacy

This section will go through the concept of privacy, its origin and what it means for the individual person. Regulations and privacy laws are discussed as well as introducing the idea of PbD and how it can aid in the implementation of information systems.

2.1.1 Definition

In 1890 the article "The right to privacy" was published by Samuel D. Warren and Louis Brandeis, one of the earliest publications regarding privacy. They defined privacy as the *"the right to be let alone"* [17]. However this was well before the rise of the computer age, a more modern definition was coined in 1970 by Allan Westin in the book "Privacy and freedom". Westin defined privacy as *"the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."* [18], meaning that the data subject should have control over their own personal information. The definition stated in the book "Privacy and freedom" has been used as inspiration for many other privacy principles and data regulation laws [19].

2.1.2 Legislation & GDPR

Privacy legislation refers to laws that deal with how PII is processed by public or private organisations, governments and other individuals. These laws serve as a crucial foundation when designing any system that handles personal data. The Universal Declaration of Human Rights says that every individual has the right to privacy [20], however different countries have their own privacy laws and the interpretation of the right to privacy may differ. Besides national privacy laws, there are also international organisations with their own privacy legal standards, such as the EU.

In 1995 EU passed the Directive 95/46/EC, which was meant to protect the privacy of the individual in each of the EU member countries [21]. The successor to Directive 95/46/EC is the more recent and modern General Data Protection Regulation (GDPR), which was implemented in 2016 to deal with the shortcomings

of the previous law. Some of the changes include being more strict with consent, mandatory breach notifications, the right to have data removed if it no longer serves a purpose or consent is withdrawn and having privacy taken into consideration when designing a system that handles information [7, 14].

GDPR consists of 99 articles and article 5-11 clarifies the fundamental principles relating to the processing of personal data, the principles are [22]:

1. **Lawfulness, fairness and transparency(article 5.1.a):** The data must be "processed lawfully, fairly and transparent in relation to the data subject". This means that the data subject must be informed of what processing that will occur, the processing must match the actual description and the processing must match one of the purposes specified in the regulation. Privacy notices and terms and conditions should be used to inform the data subject.
2. **Purpose limitation(article 5.1.b):** Personal data must only be "collected for specified, explicit and permitted purposes". Meaning that organisations must define what the data will be used for and how they limit the processing to only what is necessary.
3. **Data minimisation(article 5.1.c):** Personal data being processed should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Meaning no more data should be stored than what is necessary or required.
4. **Accuracy(article 5.1.d):** Personal data need to be "accurate and, where necessary, kept up to date". Organisations should have implemented processes and techniques that keep all personal data accurate and up to date. The data subject has the right to have the controller without delay fix inaccurate personal data or have it deleted(article 16, recital 65).
5. **Storage limitation(article 5.1.e):** Personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed". Meaning, when data is no longer needed, erase it. Data that is simply stored also goes under the definition of processing and therefore a Data Subject Access Request(DSAR) can require copies of stored and backed-up personal data.
6. **Integrity and confidentiality(article 5.1.f):** Organisations are required to process personal data "in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage". Confidentiality is the "property that information is not made available or disclosed to unauthorised individuals, entities, or processes"¹ and integrity is the "property of accuracy and completeness"².
7. **Accountability(article 5.2):** The last principle states that "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1".

¹ISO/IEC 27000:2018, Clause 3.10

²ISO/IEC 27000:2018, Clause 3.36

Article 12-23 goes into more detail of the data subject rights. Article 12 states that information must be given to the data subject "In a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child". Among other things discussed are: 1) The right to access, the data subject has the right to a copy of their personal data and the purposes of processing. 2) The right to be forgotten, the data subject can request that information is erased based on specific circumstances. 3) The right to object, the data subject can object to having its personal data processed. How personal data is processed by an organisation and the rights of the data subject are often contained in a document called privacy notice [7, 22].

2.1.3 Privacy by Design

PbD is a very important requirement of the GDPR which states that "the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures", as mentioned in article 25 [7]. Meaning that solutions to protect privacy should be taken into consideration when designing the system, instead of relying only on privacy protecting add-on features after the design phase. The concept of PbD was initially developed by the researcher Ann Cavoukian and for the first time published in a joint report in the year of 1995 [23]. In the year of 2009 the PbD framework was published, the framework consists of seven foundational principles. The purpose is to ensure privacy within an organisation information systems and to give the data subject greater control over one's information. The seven principles are [24, 25]:

1. Proactive not reactive; preventive not remedial
 - Take into consideration privacy concerns from the beginning of the design before privacy issues arise.
2. Privacy as the default
 - Personal data is protected automatically in any IT system, no action by the user is required to protect privacy since privacy is built in by default.
3. Privacy embedded into design
 - PbD is embedded into the system architecture during design and not added on afterwards, there is a mapping between privacy protected data and the system functions.
4. Full functionality - Positive sum, not zero-sum
 - Unnecessary trade-offs should be avoided, privacy should be seen as an enabler of functionality not a hinder.
5. End-to-end security - Lifecycle protection

- Data has a potentially long lifespan, data should be protected throughout its lifecycle. Stakeholders should be informed which data is transferred to and how and when data is disposed of.

6. Visibility and transparency

- Seeks to provide stakeholders with tools and information that can verify that the organisation is achieving the privacy objectives and regulatory compliance.

7. Respect for user privacy

- The interests of individual privacy are at the utmost interest. Provide notice of data collection and privacy policies, obtain user consent, ensure data is fresh and accurate, give users access to their own data.

2.2 Internet of Things systems

IoT refer to computing objects equipped with network utility which allows them to exchange data with other systems over the internet. These devices are small-scale which allows them to be integrated to home appliances like refrigerators or dish washing machines but also remote health monitoring and home automation. IoT is valuable because it simplifies and automate processes in several areas such as industry, military, society's infrastructure and organisations. It can reduce labor cost, improve service & delivery and enhance quality of life, it could very well grow to be one of the most important technologies in our everyday life. For example, altering the light, managing TVs, changing the temperature or monitoring live feeds of cameras [26].

However, because the nature of IoT devices' ecosystem, they become an attractive target for attackers. Its simplicity and convenience provokes a disadvantage in the security aspect. The restriction of processing power and sometimes lack of energy source, cause devices to concentrate most of their computing power on executing functionality, leaving a liability in the security aspect. Sensitive data is frequently being transmitted between IoT devices and systems which could be of interest for malicious users. Because manufacturers often overlook the security for performance and functionality, they are susceptible to cyber-attacks. The infrastructure of the IoT could also evolve in to an additional issue, the system is generally designed to communicate with a cloud service and a smartphone application. This creates a wider attack vector and exposes several parts of the ecosystem. The systems alone are likely to contain vulnerabilities and linked together the severity increases rapidly with. Sometimes, compromising the actual device is not the true intention of the attacker, but acquiring access to the network of the IoT device. [27]

2.2.1 Smart cameras

Video surveillance has, since 1970s, proven a useful and extensive approach to ensure security for people and goods [28]. It is limited to its own field of view based on its

placement but combining several cameras can result in a decent monitored area. Over time, with technology developing, cameras improve and are upgraded with added features and qualities. Since smart cameras (or IoT cameras) are connected to the internet, they provide a new communication aspect. Oftentimes the cameras are equipped with a speaker and microphone, and supports remote live streaming which includes two-way communication. This allows a user to have constant observation via an application, but also being able to interact through the device over voice. However, all devices connected to the internet are vulnerable to malicious intrusion. In 2018, Bugeja et al. used Shodan, a search engine for devices connected to the internet, to discover over half a million smart cameras all over the world that were leaking sensitive and vulnerable data for attackers [29].

When activating a smart camera, the user is generally required to provide PII data such as name, email and address, it might also have the possibility to link with another third party account. Streaming live feed from the camera, alerting motion detection or face recognition indicates uploading videos or pictures straight from the camera to the cloud. It is crucial that all this information is carefully managed to comply with GDPR to not risk the integrity or privacy of the users. This forces manufacturers to sharpen its security and perhaps strictly following a framework like PbD. As previously mentioned, 47% of hacking attempts in smart homes have targeted smart cameras, possibly because of its weak security [6].

2.3 Security auditing and privacy analysis

This section discusses techniques and methods that can be used to analyse security implementations in a information system, as well as methods used to analyse how good systems are at handling privacy.

2.3.1 Reconnaissance

Reconnaissance is the process of gathering information about a system and is the very first step of a security assessment. The goal of a penetration test is to find security vulnerabilities in a system. Therefore it is essential to gather as much information as possible about the system in order to identify all potential entry points that an attacker could abuse. This can be achieved by going through information such as device documentation and manuals or using search engines such as google to find online resources about a product or service. Data that can be useful are for example device components such as communication protocols used, CPU architecture, hardware ports and operating system [30]. There are also tools that can be used to extract more information about the target. For instance the open-source tool nmap can be used to scan the targets IP address in order to identify open ports and services. Another relevant method is DNS Discovery, it obtains information about domains and IP owners, such as registered owner and registered country [31].

2.3.2 Network communication

The two most common protocols used for data transmission within computer networks are TCP and UDP, they operate on the transport layer 4 of the OSI model. TCP uses connection oriented transmission, which implies that a connection is established between two endpoints before data is sent, also re-transmission and error detection are attributes of TCP to ensure reliability. TLS is often an addition on top of TCP in order to encrypt all traffic sent. UDP is preferred when transmitting streams of data such as voice and video, since it does not perform a connection establishment and thereby reduces data transmission time [32]. How devices communicate over the internet can be analysed using packet analysis tools such as tcpdump or Wireshark. Information found by these tools can for instance be IP source and destination, DNS request and response, unencrypted HTTP traffic and the use of other protocols [33, 34].

2.3.3 Android application

Most IoT devices are controlled by an smartphone application, this thesis focuses on android applications. Android applications are written in Java but has a more complex architecture unlike regular Java programs that often have a single entry point. A normal android application consist of multiple app components such as services, activities, content providers and broadcasts, these components must be declared in the file *AndroidManifest.xml*. The manifest file is very important and is used by the Android OS to route intents between the specified components. Even more important is that the manifest holds the applications permissions to use different services, e.g. CAMERA allows the application to access camera requests and *ACCESS_FINE_LOCATION* allows the application to access the user's precise location. In the end everything required for the application, including code, icons, XML files is combined and packed into Android Packages(APKs) before being distributed on platforms such as Google play [35, 36].

2.3.4 Privacy analysis

There are several studies on the subject of privacy and data leakage within IoT systems, many IoT application have been shown to leak sensitive information to unauthorised entities. Some IoT application transmit sensitive data to remote servers for profiling user behaviour and visualisation of data, meanwhile users have little insight and control over what data is shared and to whom [37–39].

Analysis of privacy related issues can be performed manually or with the use of automated tools. There are typically two different methods when using automated tools on software, static and dynamic analysis. Which are generally used for vulnerability analysis, vulnerabilities can be exploited and used to compromise the privacy of users. First, static analysis is accomplished by analysing the program code at compile time before the code is actually executed. The static analyser warns about potential bugs, security and privacy issues before the code is executed. The second method is dynamic analysis, which operates during the execution and interaction of a program. Dynamic analysis require different execution inputs in order to identify

the corresponding execution output [27]. There are several methods to discover and analyse data leaks in applications, this thesis have opted to use static analysis in the form of taint analysis. The technique simply maps the flow of data from sources to the corresponding sinks. A source is the method where input of personal data is made such as a phone number or the GPS location. A sink is the end of the data flow where a method to transmit personal data to an external party is made, such as an HTTP request. [35, 40].

2.4 Certificate Authority

Certificate Authority (CA) is a trusted organisation that provides digital certificates to verify entities on the internet. The digital certificates assures secure and trusted communication between connected parties. A valid certificate generated for a system could communicate securely with another system or device that trusts the issuer of the certificate. These digital certificates are electronic documents containing information that proves the ownership of the file. They can be generated by software and consists of a massive numerical value used for encryption or decryption. In *HTTPS*, when initiating a connection from a browser, a certificate is transferred to the server as part of the *SSL handshake* [41]. The certificate will then be verified against the server's trusted certificate authorities, if it is validated the communication is allowed between the two parties. The idea is to maintain integrity and privacy during the transmission between a server and client [42].

However, if distrusted or evil-minded certificates designed by an attacker is assigned to a device, the device could connect to the server and disguise as an authorised user if the authentication mechanism is not properly implemented. An authorised user is capable of revealing the encrypted data. This implies that a malicious, but authorised, user could intercept permitted traffic and perform a MitM attack. This requires systems to handle certificate requests correctly to avoid those types of attacks.

There is plenty of research on IoT in regards to privacy regulations and foremost the GDPR legislation. Wachter [12] identifies privacy and identifiability challenges within the realm of IoT through a literature review. More specifically four challenges: 1) How profiling methods can disclose information about users identity and their private life; 2) The control of sharing identity and sensitive data; 3) Consent and the uncertainty of the amount and value of the data; 4) Honesty, trust and transparency between the IoT manufacturer and user. It is stated that the GDPR requires more specification and implementation when it comes to the design and deployment of IoT technologies. Foremost transparency and awareness of possible risks and consequences is important for users to make an informed decision when deciding to use a service. Kounoudes et al. [13] research is built on the work of Wachter and identifies a list of GDPR compliant characteristics that can aid in future development of IoT privacy frameworks. In another publication of Wachter [43] a three-step transparency model is developed with a set of proposed guidelines. The goal is to get IoT suppliers and data controllers to be more transparent with processing of personal data but at the same time keep a balance between information disclosure and the right to privacy. Bastos et al. [44] researches privacy implications of IoT devices in regards to GDPR and potential mitigation strategy. The authors suggest the use of lightweight encryption schemes such as elliptic curves, which is more suitable for IoT devices with limited hardware capabilities. [45] suggests a method to verify GDPR compliance of IoT systems with the help of a blockchain solution. GDPR requirements such as user consent, data protection, data transfer and data minimisation can be used for verifying processing units with the help of smart contracts.

Li et al. [14] investigate how PETs can be used and implemented in the different layers of the specified four-layer IoT architecture with regards to PbD in order to reach privacy requirements of privacy legislation's. Barati et al. Chaudhuri et al. [46] designed a framework based on PbD which consist of 8 steps with the goal to protect the privacy of users in regards to IoT smart home devices. Pape et al. [47] developed a method to map privacy patterns between IoT, fog computing and cloud computing architectures. Seven different privacy patterns based on the concept of PbD was applied to smart vehicles to improve users privacy.

Another equally important research area that has strong associations with GDPR is research made on privacy policies. Shayegh et al. [48] develops a method that generates a simplified and shortened version of privacy notices which can aid users in making informed decisions about their privacy, the work was based on reviewing 25 privacy policies of IoT smart home devices. Renaud et al. [49] identifies GDPR

requirements for privacy notices and then designs a guideline for how to implement proper privacy notices that are GDPR compliant.

Security and privacy issues for IoT devices and most relevant to this thesis IoT cameras, have also been studied. Manske [11] performs an extensive vulnerability assessment of an IP camera, a total of 11 vulnerabilities were found and the author discusses potential solutions and mitigation strategies. Alhbari et al. [8] develops an IoT analysis framework which can be used to analyse the security and privacy of IoT systems, the framework was tested on 5 different camera devices. A similar study by Tekeoglu et al. [50] suggests the use of a testbed that can be used to analyse security and privacy issues for WiFi and Bluetooth connected IoT systems. The method used is to capture layer 2 and layer 3 packets and analyse the packets for different features. There are more studies [9, 10, 51] done on vulnerability assessments of internet connected cameras. However they are very similar to each other, uses a limited methodology and do not provide any solutions to the problems or suggestions on future work.

IoT devices are often controlled by an mobile application, security and privacy issues related to IoT mobile applications have been studied extensively. Subahi et al. [52] develops a tool that uses supervised machine learning to extract information from the traffic between IoT applications and the cloud, the intent is to identify sensitive information through packet sequences and the packet sizes. Konstantin et al. [53] designed a framework that is meant for threat analysis of mobile health applications, the method is used to identify common security and privacy related issues. Ferrara et al. [40] researches how static analysis methods can be used as a PET in order to ensure GDPR compliance, the authors identifies what different tools exist and how they differ in capturing information. Arzt et al. [54] developed a tool called FlowDroid which is a static taint analysis tool that can be used on android applications, the tool identifies sensitive information and maps them to where the data is leaked.

There is a lack of practical experiments and analysis of physical devices in regards to GDPR for IoT devices. Many of the related studies mostly focuses on theoretical issues or concentrates the research into particular fields within GDPR and IoT. Presently, there is a shortage of tests designed to discover IoT devices, especially smart cameras, compliance with GDPR and how a framework could potentially benefit the device. This research aims to uncover the impact a framework intended for GDPR has on IoT smart cameras data management.

This chapter describes the different processes and approaches taken for the literature review and the case study in order to answer the research questions.

4.1 Research method

A literature review was required to obtain knowledge about GDPR in general but also its role in IoT's data management. To evaluate the devices' ability to achieve GDPR compliance, it is necessary to completely understand legislation and how GDPR impacts the IoT data lifecycle. It is also important to recognise how the PbD principles implements privacy throughout the entire development process.

To classify the behaviour and security levels of these different cameras, case studies were executed that focused on evaluating their ability to properly handle sensitive data. The cases contained different penetration testing techniques and were executed in a secure test environment. By implementing case studies, more detailed data and concrete information is gathered that aids to answer the research questions.

4.2 Literature review

The literature review has two major purposes. 1) Is to find relevant literature that will strengthen the knowledge about GDPR and PbD and the role it has for IoT systems, as well as to understand what the requirements are to achieve GDPR compliance. 2) Is to identify similar studies that perform penetration tests and security auditing of IoT systems. Which aided in deciding how the test environment was to be structured as well as selecting relevant case studies that will help answer the research questions. Furthermore, a literature review will deliver an unbiased view on the state of the current research, that will ultimately strengthen the credibility of this thesis and help answering the research questions. The literature review consist of three different stages. First, planning which includes establishing selection criteria and selecting relevant keywords. Second, is the actual implementation of finding relevant literature as well as excluding and sorting. Third, is reviewing and evaluating the actual information of the literature [55].

4.2.1 Databases and keywords

The databases mentioned in the bullet point below were used to find relevant articles.

- BTH Summon
 - Is a collected database with all available literature from BTH online library, literature from the following databases where used:
 - * IEEE Xplore
 - * Springer
 - * ACM digital library
 - * EUR-lex
 - * O'Reilly
 - * ScienceDirect
- Google Scholar

The keywords used were related to the RQs in order to find relevant literature. The keywords were also divided into three categories. First category consist of general terms relevant to the thesis. Second category was based on GDPR and PbD. Third category was based on penetration tests and security auditing. The keywords was used in different combinations and are presented in Table 4.1. Once beneficial articles were gathered, the snowballing method were performed to discover more valuable papers.

General terms	GDPR/PbD	Security auditing
IoT	GDPR	Vulnerability
Internet of things	PbD	Exploit
Privacy	Privacy by Design	Penetration test
Security	Regulation	Static analysis
Camera	Law	Dynamic analysis
Framework	Privacy Enhancing Technologies	
Android		

Table 4.1: List of keywords

4.2.2 Selection criteria

Below is satisfied criteria presented for selecting relevant literature. Information not concerning the RQs did not adhere to the criteria, like introduction and background.

- Literature written in English.
- Literature not published before 2014.
- Literature of scientific origin, e.g. scientific journal or conference.
- Literature with relevant title, abstract and conclusion.

4.3 Privacy by Design and IoT device selection

This section discusses the reasoning for selected PbD principles, as well as what IoT devices were picked.

4.3.1 Selection of principles in Privacy by Design

Privacy by Design covers the process of implementing privacy in software. For this article, three principles were selected to illustrate a part of the PbD that focuses on data management. The principles are:

(2) Privacy as the Default Setting

This entails that the default setting for a user shall deliver strong protection of the data. The user should not be required to modify settings to increase privacy.

(5) End-to-End Security — Lifecycle Protection

This forces the design of the application to assure security from start to finish. When the data is collected it is preserved with caution and fully removed at the end of the process.

(6) Visibility and Transparency

This allows the stakeholders to observe and verify that the agreed upon involved operation is in fact functioning correctly. [24]

The devices' characteristics will be measured to the principles which helps to answer the research questions.

4.3.2 Selection of IoT devices

Initially different areas of IoT devices were investigated by reading similar studies evaluating privacy issues in IoT, among other medical IoT and wearable IoT [15, 16]. However these devices are in many cases expensive or difficult to acquire physically. Therefore the choice became IoT cameras that are easier to come by and more affordable, as well as being a more popular target for hackers. This project is in collaboration with the company, which is providing financial aid in purchasing the devices. The goal is to evaluate privacy issues in general on IoT cameras and the relationship it has with GDPR and PbD, however it is not feasible to analyse every single device in existence. Therefore, the idea was to select cameras with different classifications, one device known to be secure, one camera that is highly attractive on the market and one budget camera. As a result, the case study will target a wider spectrum of categories in IoT cameras. The criteria for selecting the cameras are as following:

1. Within the set price range.
2. Connected to the internet.
3. Cloud support and integrated mobile application.

Additional beneficial characteristics that was taken into consideration when selecting the devices were:

1. Devices with removable storage.
2. Devices with Linux kernel.
3. Known history of vulnerabilities or privacy issues.

After researching related work that discovered vulnerabilities in devices, the following cameras were selected that met the necessary prerequisites:

Arlo essential spotlight camera

This device is considered to be secure. The Arlo brand was originally founded by the company Netgear but is seen as an independent company since 2018 although they still have a close relationship with each other [56]. The company is highly focused on security and has a bug bounty program, which encourages and rewards developers who help create Arlo's products more secure. This typically illustrates a kind of maturity in security reasoning and transparency.

Foscam C2M IP camera

This is a popular brand which is considered to be less expensive and also has a history of security vulnerabilities [57, 58], previous vulnerabilities motivates further investigation to examine whether the company has implemented mitigation or not. The device has removable storage and the brand is known to use Linux as kernel in their devices.

Ring indoor camera

This device is considered to be one of the more popular IoT cameras, the company has a following of 135 000 subscribers on YouTube. It gained its popularity after being showcased on the TV-show shark tank presenting one of the first smart doorbells. The company was later sold to Amazon in 2018 and today provides other camera solutions as well [59]. The company has a history of having privacy related issues [60, 61] which strengthens the argument to research this device to see how it has counteracted the vulnerabilities.

4.4 Case study

The test was divided into several case studies that are identically executed for each camera within a monitored environment constructed for the tests. The case studies were designed to examine different parts of the cameras' architecture against the selected PbD principles. Each case study provides information whether or not the cameras successfully meet the GDPR requirements. The case studies are categorised into different classifications, such as; network communication, physical security, Android application and web interface. The categories and detailed descriptions of each test are presented in 4.4.3.

4.4.1 Environment setup

To better analyse the communication and investigate the devices' behaviour, an environment was established. The idea was to create a network where a computer runs a router on a virtual machine that also monitors all transmission going through. Figure 4.1 shows how the environment was set up.

The host was a laptop running Debian as a virtual machine that reroutes packets from an inner network to the internet. The Debian machine had two interfaces, *enp0s3* (EXTIF) was an external interface that provides the machine with internet, and *enx9cebe8ed9497* (INTIF) that manages the internal network. The machine runs three main services:

- Dynamic Host Configuration Protocol (DHCP) – Provides IP addresses for connected devices
- Domain Name System (DNS) – Translates domain names to IP addresses for devices surfing the internet
- Wireshark – Analyses the network traffic to see how the connected devices behaves

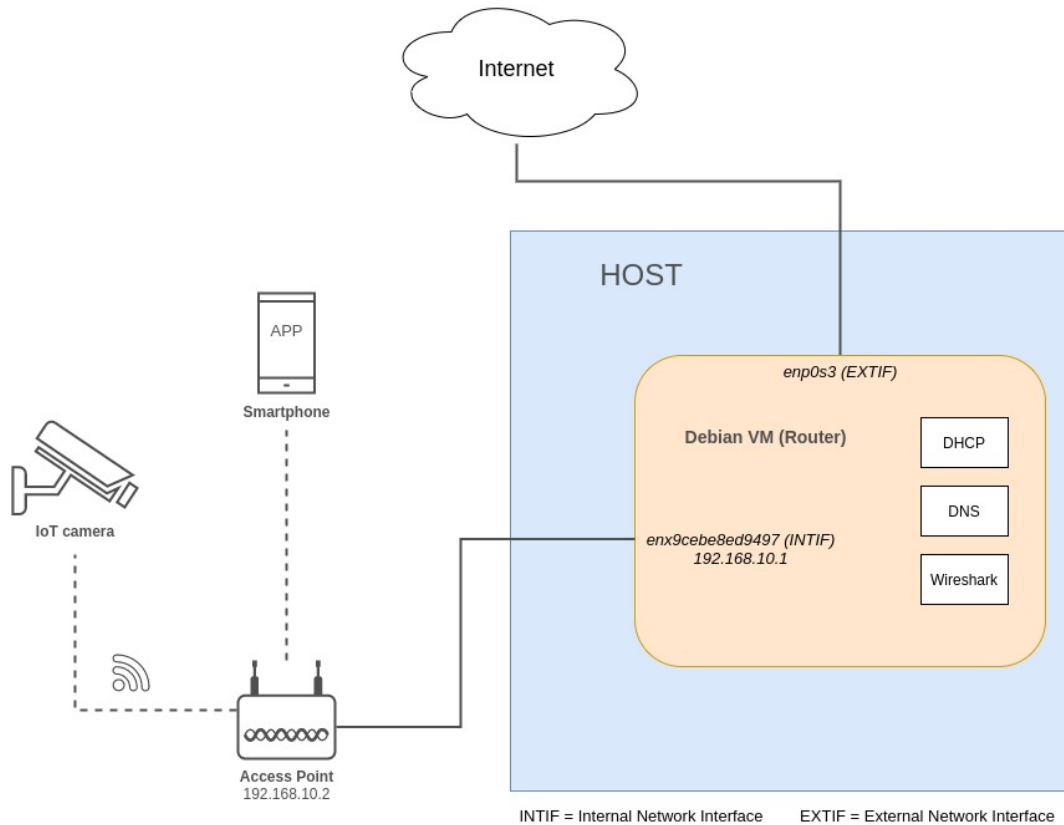


Figure 4.1: Environment Setup

The DNS and DHCP server was run with *DNS masquerade* or *dnsmasq*, it is designed as a lightweight service to provide DNS and DHCP for smaller networks [62]. Wireshark is a great tool to analyse live network traffic data in detail, it was used to dissect non-encrypted traffic to evaluate the different IoT devices functionality and protocols operated.

Since the constructed router did not offer wireless connectivity, an access point (AP) was required for the IoT devices to connect. This AP only operated to forward the wireless packets to the router, it provided no firewall or IP sharing functions [34].

The devices required an application (in this case android application) for activation and setting up the desired configuration. The smartphone required internet access to initiate the camera installation process, which forces the smartphones to connect to the router immediately. The applications' functionality varies from camera to camera, but each one provides a cloud storage service. The cloud storage is partly responsible to collect motion detection alerts, motion detection images and saved video streams. The application is downloaded on the authors' smartphones to simulate real consumer usage. An overview of the environment and the devices is shown in the tables below.

Router	
Hardware device	Dell XPS 13
Operating system	Debian 10 (Virtual Machine)
DNS & DHCP	dnsmasq 2.80
Network sniffer	Wireshark 2.6.20
Internal interface (LAN)	enx9cebe8ed9497 (INTIF)
External interface (Internet access)	enp0s3 (EXTIF)
Access Point	
Hardware model	ASUS RP-N12
Operation Mode	Access Point
Operating Frequency	2.4G Hz
Technical Standard	IEEE 802.11bgn
IoT Cameras	
<i>(Comprehensive information below)</i>	
Arlo	Essential Cam
Ring	Indoor Cam
Foscam	C2M Cam
Android Applications	
Arlo 3.2_28350	82 MB
Ring Always Home 3.38.1	124 MB
Foscam 2.7.0	56 MB

Table 4.2: Environment details.

Arlo essential Specifications	
Camera Resolution	1080p HD
Power Supply	6 months chargeable battery
Connectivity	2.4GHz Wireless 802.11 b/g/n
Audio Specs	Two way audio
System Requirements	iOS 11 or Android 5.0
Size	3.5 x 2.0 x 3.0 in (89 x 52 x 78.4 mm)
FCC ID	*****09

Table 4.3: Arlo specifications

Ring Cam Specifications	
Camera Resolution	1080p HD
Power Supply	Indoor power cable
Connectivity	2.4GHz Wireless 802.11 b/g/n
Connection Speed	Requires a minimum upload speed of 1Mbps, but 2 Mbps is recommended for optimal performance
Audio Specs	Two way audio with noise cancellation
System Requirements	iOS 9.3x or later, Android 5.0 or later
Size	1.81 in. x 1.81 in. x 2.95 in. (46 mm x 46 mm x 76 mm) (without stand)
FCC ID	*****01

Table 4.4: Ring specifications

Foscam C2M Specifications	
Camera Resolution	1080p HD
Power Supply	Indoor power cable
Connectivity	2.4G: IEEE802.11b/g/n & 5G: IEEE802.11a/n/ac
Audio Specs	Two way audio
System Requirements	N/A
Size	70x70x120 mm
FCC ID	*****2M

Table 4.5: Foscam specifications

4.4.2 Tools and techniques

This section explains the different tools and techniques practiced throughout the different stages of the case studies.

Data gathering

First the use of Open Source Intelligence (OSINT) is manually used to collect valuable information about the devices, sources such as user manuals, vulnerability reports

and other public records. Second the following tools were used to gather OSINT data:

- Whois: Delivers information about internet resources such as domain names or IP addresses [63].
- Nslookup: Retrieves IP addresses associated with domain names [64].
- IP geolocation: Pairs the IP address to a geographical location [65].
- fccid.io: All IoT devices have a unique FCC id, the service examines various documents connected to a device [66].

Another method utilised is port scanning, nmap is a flexible open source network utility tool that scans devices or networks for open ports and running services. It provides detailed information of what each host is offering in terms of operating system, firewall filters and more attributes. [67]

Vulnerability analysis and exploit

From the previously mentioned scan, the result was manually analysed and researched based on known vulnerabilities to find possible exploits. Additionally, automated tools and nmap scripts scanned the system for vulnerabilities. OWASP ZAP [68] is a tool that automatically scans for vulnerabilities on the webserver, as well as intercepting and altering packets sent to the webserver. Also, OWASP ZAP was used as a proxy between the IoT webserver and a webserver that was manually set up in order to test the use of a self-signed CA. Found vulnerabilities are exploited if possible.

Analysis of android application

In order to examine the code of an android application file with '.apk' extension, the first step was to use an archive extractor. This generated one or more executable files that are compiled with the '.dex' (Dalvik Executable) extension. Next the '.dex' file can be converted into a '.jar' file using the tool Dex2Jar [69]. By now the source code of the android application can be read using a Java decompiler such as JD-GUI [70]. The source code was manually examined for security and privacy issues, however there was a tremendous amount of code and there are automated tools that can aid in some areas:

- Androguard: Extracts permissions and activities [71].
- Mallodroid: Finds faulty SSL implementation [72].
- FlowDroid: Finds leakage of sensitive information [54].
- APKLeaks: Scans for URIs, endpoints and secrets [73]

Other methods consisted of extracting strings to identify encryption algorithms used, communication with IP addresses, the use of cloud services and databases.

4.4.3 Case studies

This section describes the case studies purpose, method and examines what impact it has on PbD principles. Case studies 1, 2, 4, 5, 6, 7, 8, 9, 10, and 13 provides information necessary to answer RQ1. The outcome of case study number 3, 11, 12 and 14 will help answer RQ3. Finally, all case studies will contribute to answer RQ2 to different extents. The motivation behind the selection of the test cases is based on previous studies found in the literature review and developed frameworks. The idea is to test the whole IoT systems in close correlation with GDPR, which includes the network communication, physical device, android application and required GDPR instruments such as DSAR.

Each case study is assigned with a severity value between 1-3. A lower severity level indicates that the case has the potential for critical privacy and security issues related to the GDPR. Meanwhile a higher value is considered a minor impact on privacy and security related issues in regards to GDPR. For example a case closely connected with sending PII information between different entities has the potential to disclose sensitive information, this case would be considered of highest priority severity level 1. On the contrary for a case such as checking if privacy settings exist in the android application, this is good practice for a company and shows transparency. However it is not a necessity and would not have any critical impact on the PII being processed of users, therefore this case is considered of lowest priority.

The bullet points below describes the content included in table 4.6 which presents an overview of all case studies.

- **Severity:** A number that illustrates how severe each case potentially is.
 - **Severity 1:** Critical impact - Potentially leading to severe privacy issues by leaking sensitive information about users or disregarding GDPR obligations.
 - **Severity 2:** Major impact - Security issues that has no direct connection with PII but has the potential to further lead to privacy issues of the users.
 - **Severity 3:** Minor impact - Methods used to observe functionality of the IoT systems or observing recommended technologies and methods from the GDPR, which are not strictly enforced by the GDPR.
- **Category:** The part of the system the test is targeting
- **PbD principle:** The PbD principles the test may have an impact on.
- **Description:** Short summary description of the test.

#	Category	Description	PbD	Severity
I	Network communication	Monitor camera's communication at activation	2 & 5	3
II	Network communication	Monitor camera's while interacting with smart phone application	2 & 5	3
III	Network communication	Identify IP addresses' source location, are there any contradictions with the privacy policies?	6	1
IV	Network communication	Verify unnecessary ports open or out of date services running	2	2
V	Network communication	Investigate susceptibility to unauthorised certificates with self-signed SSL certificate	2 & 5	1
VI	Physical security	Information disclosure, possibility to reset camera to unsafe state, removable storage	2 & 5	2
VII	Physical security	Examine exposed serial ports for weak authentication mechanisms	2	2
VIII	Web application	Password policies and brute-force protection, vulnerability scan	2 & 5	2
IX	Android Application	Check for faulty SSL implementation	2 & 5	2
X	Android Application	Identify implemented encryption in the android application	2 & 5	2
XI	Android Application	Verify privacy policies and settings in application	6	3
XII	Android Application	Compare permissions in the manifest and the features of the application to identify if the application is overprivileged.	6	2
XIII	Android Application	Use FlowDroid for taint analysis	2 & 5	1
XIV	GDPR	Perform a Data Subject Access Request to obtain a copy of data being processed on user	6	1

Table 4.6: Test description overview

Case study I

Category: Network communication

PbD principle: 2 & 5

Description: Monitor camera's communication at activation.

Severity: 3

This test was designed to analyse what network connections the camera attempts at first activation. If the cameras would have performed an irreversible action, it could have denied the opportunity to investigate or interact with that phase. This

was achieved by observing *Wireshark* from the constructed router explained in 4.1. By filtering out DNS requests in Wireshark and connecting the camera to the router before providing it access to the internet, DNS requests would be resent since no response was returned. The requests could then be examined to detect any suspicious or illegal activity.

PbD principle 2 demands that no user interaction should be required to protect personal data and principle 5 forces the data to be preserved from its generation to removal. By exploring the first internet connection and activation of the camera, Wireshark could reveal if there is any sensitive data transferred in plain text.

Case study II

Category: Network communication

PbD principle: 2 & 5

Description: Monitor camera's while interacting with smart phone application.

Severity: 3

Similarly to the previous case study, this analyses transmitted network traffic, however, it focuses on mobile application interaction. Depending on the camera, the phone app has plenty of functionality that possibly could affect users' privacy if not managed correctly. Account information with PII is accessible on the application as well as live streaming straight to the device. By studying how this data is being handled, it is possible to recognise how the cameras comply with GDPR. GDPR requires the streaming data and motion detection photos which are saved, to be stored on a EU server or to notify the user if it will be stored outside the EU. It is also a necessity for the PII to be safely stored and communicated over the internet.

To inspect the data exchange between the devices, both the camera and mobile phone were set up on the monitored test environment. This allows Wireshark on the router to successfully interpret all messages going from and to the phone and camera. The traffic is then studied to ensure it complies with PbD principle 2 and 5, which forces default protection of integrity and assures the traffic can not be tampered with.

Case study III

Category: Network communication

PbD principle: 6

Description: Identify IP addresses' source location, are there any contradictions with the privacy policies?

Severity: 1

To ensure no illegitimate communications with unfamiliar IP addresses was active, every IP's geolocation was inspected to guarantee the manufacturers comply with their privacy policies. Several websites offer this feature but [65] was used for this purpose. A simple search of the IP address provides information like: country, region, city and organisation.

PbD principle 6 requires enterprises to be transparent with their data management, this suggests that no remarkable connections to unknown locations should be estab-

lished without user's consent.

Case study IV

Category: Network communication

PbD principle: 2

Description: Verify unnecessary ports open or out of date services running.

Severity: 2

Old services and open ports are attractive entry points for malicious users to attack, if an attacker obtains access over a vulnerable service or port, serious damage could affect the privacy of the user or functionality of the system. It is highly important of the manufacturer to ensure good protection of the system without user interaction to avoid unwanted incidents.

A comprehensive scan with nmap was performed to detect open ports on the cameras. If there were open ports present, the services running were investigated and examined for vulnerabilities manually and with nmap scripts.

PbD principle 2 entails systems being secured by default. If a device is running legacy version services, they could be vulnerable to exploits. Unused or insecure ports are also a gateway for attackers to enter a system.

Case study V

Category: Network communication

PbD principle: 2 & 5

Description: Investigate susceptibility to unauthorised certificates with self-signed SSL certificate.

Severity: 1

By inserting self-signed certificates to a system, an attacker could circumvent the valid certificate restrain and disguise as an authorised user. This allows the attacker to decrypt intercepted encrypted traffic which could expose legitimate user's integrity. When applying the self-signed certificate, the response from the camera could determine whether or not it is susceptible to a MitM attack through certificates. A properly implemented system would refuse the self-signed certificate and reply with a *Bad Certificate* message, where as a poorly implemented system would in some cases only reply with *Unknown CA*.

Once the systems were tested, a *Unknown CA* response entailed misuse of CA handling. A new webserver was established with self-signed certificates to simulate a functional HTTPS server. ZAP operated as a proxy between the newly created webserver and the IoT camera to monitor, analyse and manipulate the traffic. Rerouting *iptables* and *dnsmasq* rules to the ZAP proxy was required for the proxy to function accordingly.

By allowing circumvention of the CA with self-signed certificates, the system is not ideally handling SSL connections by definition. This indicates a breach on the PbD principle 2 which enforces privacy by default and the PbD principle 5 end-to-end security can not be achieved. PbD 5 requires the user to be informed of how the

data is managed and which whom has access to the data, in a MitM attack the user is most likely unaware of the attacker's control over the data.

Case study VI

Category: Physical Security

PbD principle: 2 & 5

Description: Information disclosure, possibility to reset camera to unsafe state, removable storage.

Severity: 2

This case study explores what physical vulnerabilities are exposed by the cameras. What information an attacker could gain by accessing the actual device. If it was possible to abduct removable storage, reset the camera to unsafe state which could possibly be exploited or discovering sensitive information for mischievous use. The United States Federal Communications Commission designates a FCC ID to all devices which is a unique identifier. By looking up the FCC ID of a selected IoT camera, an attacker could acquire detailed knowledge about the device and its functionality on a complex hardware level. This data is not classified and not necessary sensitive, but could however be seen as a great source of information for reconnaissance.

A thorough physical inspection of the cameras was enough to discover these types of vulnerabilities. By presenting excessive information, it could contradict PbD principle 2, since the device is not necessarily avoiding exposing of potentially sensitive data.

Case study VII

Category: Physical Security

PbD principle: 2

Description: Examine exposed serial ports for weak authentication mechanisms.

Severity: 2

If the cameras are equipped with physical ports, there is a likelihood that they are poorly protected with weak authentication methods or security measures. Connecting cables to physical ports could provide an attacker with data or access to the device for malevolent use. Similarly to Case study VI, a thorough inspection of the device is sufficient to identify physical ports for examination.

If the ports are designed with weak security measures which allows malicious users to simply connect a cable and circumvent or trespass the authentication in some way, PbD principle 2 is not attained. The device can neither ensure PbD principle 5 which assures end-to-end protection.

Case study VIII

Category: Web application

PbD principle: 2 & 5

Description: Password policies and brute-force protection, vulnerability scan.

Severity: 2

This case study explores several aspects of the web application. It examined running web applications on the cameras to detect password vulnerabilities such as lack of brute-force protection. The server is based locally on the camera and would most likely only be threatened from a MitM attack.

Manually testing strong password enforcement by inserting different variations of letters, numbers and characters to distinguish an approved and safe password to a weak rejected password.

DirBuster is a tool that crawls a webserver's files and directories to detect hidden web pages. It was used to brute-force the server based on a file listed with common directories to identify possible vulnerabilities on the website.

BurpSuite's automated vulnerability scans was executed to detect common webserver vulnerabilities.

These different approaches evaluates whether PbD principles 2 and 5 are achieved. Default configuration shall ensure privacy protection without user's assistance and end-to-end encryption shall not allow an attacker to access sensitive information even locally on a device.

Case study IX

Category: Android Application

PbD principle: 2 & 5

Description: Check for faulty SSL implementation.

Severity: 2

By labeling the SSL implementation and its vulnerabilities, possible attacks could be executed targeting this procedure such as MitM. Absent integrity- or replay protection, or deficient encryption could lead to a MitM attacker to access and modify PII or other data being transmitted. A tool called MalloDroid was utilised to discover defective certificate validation for SSL in android application.

Allowing MitM attacks would violate PbD principle 2 & 5. Even if the vulnerabilities lie on the android application, it will affect the overall systems security. Number 5 ensures end-to-end protection which can not be fulfilled if the communication between the devices are manipulated by an attacker. This also implies that the default security is unsatisfactory which violates number 2.

Case study X

Category: Android Application

PbD principle: 2 & 5

Description: Identify implemented encryption in the android application.

Severity: 2

Establishing the encryption used by the application could help determine how it would be possible to penetrate or not. However, identifying the encryption is not necessary a violation to the GDPR. But GDPR encourages the use of the latest encryption methods and disallows vulnerable out-dated algorithms and technologies.

By observing the source code, it was possible to manually detect cryptography algorithms and their configuration. String search was performed on the ARM library files of the extracted APK files, in order to identify encryption and hash methods that had possibly been implemented with the help of native library functions. The string output search was compared against relevant keywords such as 'AES', 'RSA', 'DES', 'MD5' and 'SHA2'. The findings was compared with the *OWASP Mobile Testing Guide - Cryptography in Mobile Apps*[74] which acts as a cryptography best practice for android applications.

Case study XI

Category: Android Application

PbD principle: 6

Description: Verify privacy policies and settings in application.

Severity: 3

Article #12 in GDPR encourages systems to be transparent with their intentions of data processing and having that information easy accessible for users. Like providing the enterprise's privacy policies directly on a system or mobile phone. [48] mentions that companies often either completely incorporated the privacy notice and policies without the option to opt out of any functionality. Therefore manually investigating if there is a link to the privacy policy in the application and if it is possible to change some privacy settings is a relevant case.

Case study XII

Category: Android Application

PbD principle: 6

Description: Compare permissions in the manifest and the features of the application to identify if the application is overprivileged.

Severity: 2

Demand more access to a phone than required suggests that the application might be overprivileged. This occurs when the mobile phone exposes more parts of its system than necessary because the application has asked for more permission than required to carry out its tasks. For example, Google Maps might ask for your *GPS location* for better user experience. However, an application where you type TODO lists, is perhaps amplifying the permission by asking for *GPS location* since it is not a fundamental part for the application's purpose. An application should not request more permissions than absolutely required for its intent, it only raises questions on why that data is being saved and could expose a greater integrity risk if the app would be compromised.

Androguard performed the extraction of permissions from the android application, once obtained the permissions must be compared to the application's functionality. If unnecessary permissions exists, it is likely to be overprivileged. This could reduce the credibility of the manufacture's intent and decrease the transparency and visibility of the organisation which negates PbD principle 6.

Case study XIII

Category: Android Application

PbD principle: 2 & 5

Description: Use FlowDroid for taint analysis.

Severity: 1

The tool FlowDroid is used on all three applications, the tool identifies sources of tainted information and maps the data to their corresponding sinks. Data in source code is considered tainted if it comes from an insecure *source* such as user input, the network or a file. A *sink* is the end of the data flow where a function handles data for external sources, such as HTTP requests or sending a text message. If a source then leads to a sink, a sort of vulnerability is detected. A malicious user aware of how the source and sink are connected in the software, can tweak the behaviour after desire. The tool is designed to flag all tainted data that is passed to a sensitive sink [54]. How much and the type of data each application leaks can then be compared and analysed.

Case study XIV

Category: GDPR

PbD principle: 6

Description: Perform a *Data Subject Access Request* to obtain a copy of data being processed on user.

Severity: 1

By law, companies are obliged to provide a user with all data collected on that user within a total of 90 days, but are required to answer within 30 days according to GDPR Article 15. Alongside the actual data, the companies are obligatory to provide information about why the data is saved, what it is being used for, who has access to the data and so on. Since it is near impossible for a user to ensure removed data from a cloud service is truly deleted, this case study would act as an extra guarantee that the data is wiped.

For all smart cameras, streams and photos are uploaded to respectively cloud service with documentation of date, time and format. After a while, some content is removed from the cloud, also documented, and when successfully deleted, a DSAR is delivered. The response from the request is compared to the actual content on the cloud service together with the deleted content. This way, if the response adhere to the documentation, it signifies that the data was managed properly. Which indicates that the manufacturers are complying with GDPR in this condition. Also, by granting users information about how their data is being handled shows transparency, which satisfies PbD principle 6.

4.4.4 Privacy notices and consent forms

In order for a company to achieve GDPR compliance there are certain information the customer needs to be informed about, the customer needs to give their consent

to how their data will be processed. The GDPR contains 99 articles that needs to be followed to ensure compliance. Furthermore are there 173 recitals, even though recitals are not strictly legally binding on their own they provide context and deepens the information of the articles. In some cases certain information is not strictly required to be mentioned but encouraged by the GDPR in order to show transparency and fairness of how data is processed by a company. This information is most often found in a document called privacy notice but can exist in other consent forms as well. Based on information found from the actual GDPR legislation, foremost *Article 13 - Information to be provided where personal data are collected from the data subject*, as well as the book: *EU General Data Protection Regulation (GDPR) - An implementation and compliance guide*[7, 22], 12 different cases was picked with information that should be present in the privacy notice. In the left column of table 5.2, the actual question if certain information is present is asked and in the right column is the corresponding GDPR article/recital that discuss that subject. The following questions are used when analysing each companies privacy notice:

Privacy notice questions	
Questions	GDPR article
What personal data is collected?	Article 5.1a, Recital 39
When is personal data collected?	Article 5.1a, Recital 39
What techniques are used to protect personal data?	Article 32
Which third parties are personal data shared with?	Article 13.1.f
What the data will be used for and how processing is limited to only what is necessary?	Article 5.1.b, Article 13.1.c
Is personal data collected “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”?	Article 5.1.c
What is said about confidentiality and integrity?	Article 5.1.f
Is the data subject informed about their right to lodge a complaint with a supervisor authority against the controller?	Article 77, article 13.2.d
When data is transferred to a country outside EU or an international organisation, is the data subject informed of the safeguards put in place relating to this transfer?	Article 45, Article 13.1.f
Is the data subject informed about their right to “request if their information is rectified, removed or that its processing is restricted by the controller”?	Article 16
Is the data subject informed about their right to “object to data processing”?	Article 21
Is the information provided “In a concise, transparent, intelligible and easily accessible form, using clear and plain language”?	Article 12.1

Table 4.7: Privacy notice information

This chapter presents the findings of our research. First the result from the literature review is shown followed by the result from the executed tests, it displays each case study together with an explanation of the results.

5.1 Literature review results

The literature review was performed to aid answer the RQs of this research. Since the concept of PbD should be taken into consideration when complying with the GDPR legislation it is often discussed in research papers focused on GDPR. Therefore the reviewed papers was divided into sections based on answering RQ1 which has to do with security and privacy testing, secondly RQ2-3 which has to do with GDPR and PbD. The number of research papers in regards to which RQs they are associated with is shown in 5.1. There were two papers discussing the use of static analysis for ensuring GDPR compliance and finding IoT vulnerabilities and therefore touching on all formulated RQs.

Amount of research papers	RQ 1	RQ 2-3
13	X	
12		X
2	X	X

Table 5.1: Papers based on RQs

The literature reviewed can be divided into different categories based on their main subject. The different categories are displayed in the bullet point below. Although as previously mentioned some of the papers touches on multiple subjects, in most cases this is true for C3-C5. An overview of the reviewed literature can be found in Table 5.2. By investigating previous research, valuable information was obtained which truly aided in the design of the case studies. Information such as, what tools previous researchers used to look at privacy and security issues in foremost the android application but also methods used for analysing network traffic, how to look at privacy based on privacy persevering frameworks and the role GDPR and PbD has in the design and operation phase of IoT systems.

- **C1 - Security and privacy testing of IoT devices:** The main focus was to find research doing security and privacy test foremost on IoT cameras. Furthermore find research on frameworks for testing the security and privacy of IoT devices.
- **C2 - Security and privacy testing for android applications:** The first focus was to find research doing security and privacy test on android IoT applications. As well as finding research that suggests automated tools that can aid in analysing the android applications.
- **C3 - GDPR:** This category is targeted on finding research that discusses GDPR in correlation with IoT systems. First of, to identify what is required for IoT systems to reach GDPR compliance and secondly if something more should be included or discussed.
- **C4 - PbD:** This category is for research that looks at how PbD can be implemented to strengthen the privacy of IoT systems.
- **C5 - Privacy notice:** This category is for literature that research the state of privacy notices either in correlation with GDPR or IoT.

<i>ID</i>	<i>Comment</i>	<i>Reference(s)</i>
C1	Three papers researching security frameworks and four papers doing security tests on IoT cameras.	[75] [8] [50] [11] [9] [51] [76]
C2	One paper focused on cryptography usage in android apps. One paper with focus on security tests of android apps. Two papers researching static analysis methods and one researching dynamic analysis. One paper about user behaviour and sensitive information in IoT-app traffic.	[77] [53] [54] [78] [79] [52] [27]
C3	Seven papers with focus on GDPR in correlation with IoT systems and one paper on static analysis for GDPR compliance.	[43] [14] [80] [45] [40] [44] [13] [12]
C4	Two papers on applying PbD to IoT systems and one discussing privacy methods for systems in general.	[47] [81] [46]
C5	Two papers on implementing good privacy policies in regards to GDPR or IoT systems.	[49] [48]

Table 5.2: Researched literature overview

5.2 Summary of security assessment

This section highlights the most important findings for each camera system, a complete overview of all case studies is found in section 5.3.

5.2.1 Arlo

Arlo mostly communicates with Amazon servers (Appendix A) established in Ireland with sensitive information stored in the EU. The camera has neither physical ports or local ports available, the traffic is transmitted straight to cloud services. The device is not susceptible to self-signed CA attacks and all communication is encrypted with TLS.

Examination indicates RSA and AES encryption techniques in the application and no faulty SSL implementations were detected. Required permissions are listed in Appendix B, the device demands Bluetooth permissions although the camera does not offer Bluetooth connectivity. However, other Arlo devices support Bluetooth communication. The taint analysis with FlowDroid detected 12 leaks from five different methods displayed in figure 5.5.

Arlo responded to the DSAR after six days with a PDF containing customer information, device information, support contact and an overview of data with a diagnostic tool. However, no information or data about stored and removed video content.

5.2.2 Ring

Ring's most common connection were established to Ring-owned domain names, and the majority of its communication is with Amazon servers (Appendix A). Sensitive data is stored on Amazon servers located in Ireland. No local ports were running services and the device is not equipped with physical ports like serial ports or USB, which means it communicates directly with a cloud service using TLS. The camera does not respond to self-signed CA certificates with intentions to breach the system.

The Ring Always Home application presents the user with privacy policies and settings alternatives, it is implemented with RSA and AES encryption algorithms. A SSL certificate scan indicates signs of a certificate signed with SHA1. The taint analysis discovered 52 leaks but was unable to identify what methods they originated from. A list of all permissions requested by the application can be seen under Appendix B.

The DSAR response was received within GDPR's time limit and contained comprehensive information about different events, linked accounts, location flows and all streams and photos stored on the cloud server.

5.2.3 Foscam

The camera is susceptible to local MITM by inserting a self-signed certificate that allows an attacker to observe encrypted traffic in clear text such as the MAC address, secret key variables and the raw data of an image. It is not equipped with any physical ports, however, some local ports are running services shown in figure

5.4. The webserver does not demand any complex password policies and it has no mechanics to protect against brute-force attacks. Most communication is towards Amazon cloud servers located in USA and some in Europe. All traffic passing the router is secured with TLS to protect against cyber-attacks.

The Foscam application requires several permissions all listed in Appendix B. The taint analysis reported over 150 leaks in the android application, with some of the data being collected was not being disclosed in the privacy policy. These leaks are included in the methods displayed in figure 5.5.

Foscam responded to the DSAR in two days and it consisted of account information, device information, video alert captures and the actual videos and motion detection captures.

5.3 Case studies result

5.3.1 Case study I

Description: Monitor camera's communication at activation.

The network traffic from and to all cameras was encrypted using TLS 1.2, therefore there is no real evidence of how the devices behave. However, dns is un-encrypted which means it is possible to observe what connections the devices attempted to complete. Table 5.3 illustrates the result of all DNS requests made during the setup for the embedded software.

All devices communicated with some variance of NTP servers which have been removed from the table since they bring nothing of interest. In general connections seemed to be towards the companies different servers or to external cloud services.

<i>Arlo</i>	<i>Foscam</i>	<i>Ring</i>
updates.arlo.com	p2p-foreign1.myfoscam.com	iperf.ring.com
vzweb43-prod.vz.netgear.com	ts-foreign5.myfoscam.com	fw.ring.com
deviceapi.messaging.arlo.com	security-api.myfoscam.com	time-us.prdrings-solutions
arlostatic-z1.s3.amazonaws.com	nist1.symmetricom.com	ps.ring.com
arlostreaming-prod.ar.arlo.com	push-access.myfoscam.com	
registration.arloxcld.com		

Table 5.3: DNS request made by devices

5.3.2 Case study II

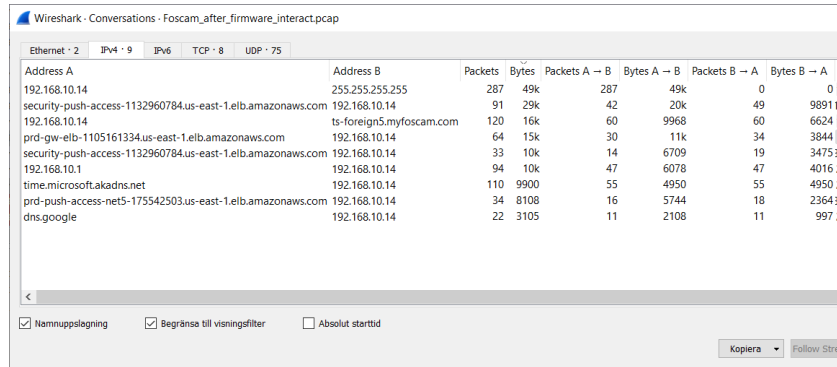
Description: Monitor camera's while interacting with smart phone application.

Similarly to the previous test, it is difficult to determine how the device operates in the network because of the encryption. However the amount of data being sent between various endpoints can be seen in Wireshark as illustrated in figure 5.1.

Arlo communicated with 16 different IP addresses whereas the majority of data was transferred between the camera and four different IP addresses, all being Amazon cloud servers located in Ireland.

Foscam communicated with 8 different IP addresses whereas the majority of transmissions were directed towards three IP addresses. Two being Amazon cloud servers located in USA, Virginia and a server from Fdcservers in Netherlands.

Ring had conversations with 15 different IP addresses whereas the majority of transmissions established was with three IP addresses. One server hosted in Ireland by Ring and two Ring owned servers located in Virginia, USA.



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
192.168.10.14	255.255.255.255	287	49k	287	49k	0	0
security-push-access-1132960784.us-east-1.elb.amazonaws.com	192.168.10.14	91	29k	42	20k	49	98911
192.168.10.14	ts-foreign5.myfoscam.com	120	16k	60	9968	60	6624
prd-gw-elb-1105161334.us-east-1.elb.amazonaws.com	192.168.10.14	64	15k	30	11k	34	3844
security-push-access-1132960784.us-east-1.elb.amazonaws.com	192.168.10.14	33	10k	14	6709	19	3475
192.168.10.1	192.168.10.14	94	10k	47	6078	47	4016
time.microsoft.akadns.net	192.168.10.14	110	9900	55	4950	55	4950
prd-push-access-net5-175542503.us-east-1.elb.amazonaws.com	192.168.10.14	34	8108	16	5744	18	2364
dns.google	192.168.10.14	22	3105	11	2108	11	997

Figure 5.1: Wireshark conversations

5.3.3 Case study III

Description: Identify IP addresses' source location, are there any contradictions with the privacy policies?

All network transmission was saved in to .pcap files and all IP addresses that conversed with the camera devices were extracted and later used to identify the location and organisation behind the IP address. A complete overview of the result can be found in Appendix A.

In total, the Arlo camera communicated with 30 separate IP addresses, the majority of conversions being with Amazon cloud servers in Ireland. With a few exceptions being with servers from Akamai technologies in Sweden.

The Foscam camera communicated with 24 different IP addresses, most of being Amazon cloud servers in USA and a few in Europe. With the exception of one server in the Netherlands belonging to the data center FDCServers.net, as well as one server in Germany belonging to the cloud service Leaseweb.

Various interaction on the Ring application caused the camera to communicate with 43 IP addresses located mostly in USA. All servers are connected with Ring in some way, hosting on amazon-ring servers. The majority of the servers originated from amazon in USA with 32 server and 11 EU servers, also run by amazon.

All three companies mentions the possibility of personal data being transferred to countries outside EU such as to USA in their privacy notice.

5.3.4 Case study IV

Description: Verify unnecessary ports open or out of date services running.

Nor Arlo or Ring camera were running any services locally. However the Foscam had a number of running services shown in Table 5.4. Lighttpd on port 88 is a local flexible lightweight webserver, it is designed to be efficient and high performance [82]. Further investigation of this service is shown in Case study VIII. Https on port 443 is the service running TLS and communicating with external sources. GSOAP on port 888 is a software development toolkit used for XML web services [83]. RTSP (Real Time Streaming Protocol) is a protocol designed for the delivery of live audio and video data [84]. RTSP service can be accessed unauthenticated, meaning anyone can see the live stream or with the use of two different authentication methods, basic and digest. Basic authenticated is considered to be less secure and can sometimes be bypassed using exploits, on the contrary digest is the more secure solution. Figure 5.2 shows the authentication method digest being used by the service. The unknown service on port 40681 was manually investigated using the tools telnet and netcat to interact with the port, however no further information was gained.

<i>Port</i>	<i>State</i>	<i>Service</i>
88	Open	lighttpd
443	Open	SSL/HTTPS
888	Open	GSOAP
40681	Open	Unknown
65534	Open	RTSP

Table 5.4: Foscam: Running services on the camera device

```
DESCRIBE rtsp://192.168.10.14:65534 RTSP/1.0\r\nCSeq: 2\r\n\r\n
RTSP/1.0 401 Unauthorized
CSeq: 2\r\n\r\n
Date: Wed, Mar 31 2021 13:37:10 GMT
WWW-Authenticate: Digest realm="Foscam IPCam Living Video", nonce="e748b9de3e5cf970b1c1d08686f7e8bc"
```

Figure 5.2: Foscam: RTSP authentication method

5.3.5 Case study V

Description: Investigate susceptibility to unauthorised certificates with self-signed SSL certificate.

Both of the Ring and Arlo cameras were implemented with security measures that only allows trusted certificates. Therefore using a self-signed certificate returned the response *Bad Certificate*.

The Foscam however, did not verify the certificate for three different URIs, meaning that we could see some parts of the data being sent in cleartext. The transmitted

traffic had to do with motion detection alerts. Sensitive information such as the device MAC address, the raw data image of a screen capture from the camera and a secret key variable was identified. An example of a packet sending the raw image in cleartext is shown in Figure 5.3. Although there was more traffic being sent excluding the three URIs presented below, these connections did not accept the self-signed certificate and a response of *Unknown CA* was noted in Wireshark as shown in Figure 5.4

- api.myfoscam.com
- push-access.myfoscam.com
- richmedia.myfoscam.com

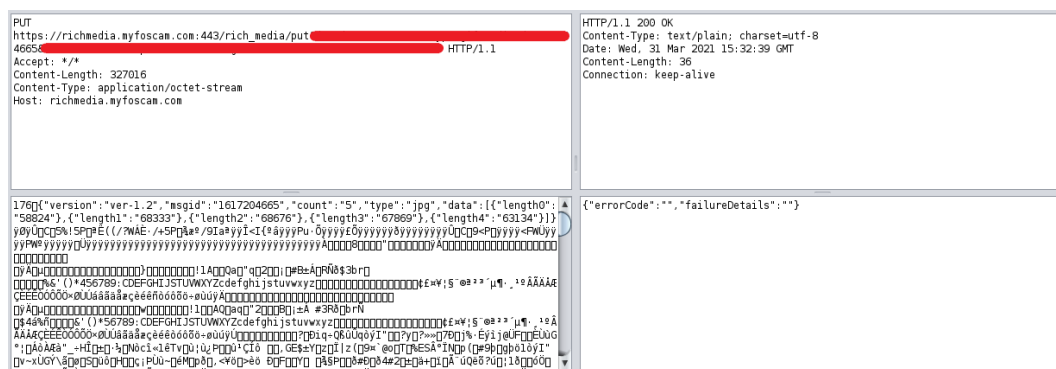


Figure 5.3: Foscam: Encrypted traffic shown in cleartext

2656	285.8335729	192.168.10.14	192.168.10.1	TLSv1.2	61 Alert (Level: Fatal, Description: Unknown CA)
2657	285.8338126	192.168.10.1	192.168.10.14	TCP	54 443 → 34701 [FIN, ACK] Seq=2992 Ack=301 Win=64128 Len=0
2658	285.9162588	192.168.10.14	192.168.10.1	TCP	60 34701 → 443 [FIN, ACK] Seq=301 Ack=2993 Win=19584 Len=0

Figure 5.4: Foscam: Unknown CA response

5.3.6 Case study VI

Description: Information disclosure, possibility to reset camera to unsafe state and removable storage on the physical device.

No camera exposes sensitive information. However both the Foscam and the Ring camera exposes the FCC ID which is placed on the physical device, only Arlo keep this information hidden within the application under device information. The Foscam camera and Ring cam has the possibility to reset the camera with a physical button to factory settings, consequently this will lead to the camera not working and it requires to go through the set-up phase again. Foscam was the only camera equipped with removable storage, a micro SD slot is located on the device. The camera provides the opportunity to store video streams and photos straight to a SD card.

5.3.7 Case study VII

Description: Examine exposed serial ports for weak authentication mechanisms.

Because none of the devices were equipped with serial ports and disassembling the device is out of scope, this case study could not be accomplished.

5.3.8 Case study VIII

Description: Password policies, brute-force protection and vulnerability scans of the web application.

Only the Foscam device had a running web application that could be used to interact with the camera. The webserver does not provide any protection against brute-force attacks, also the password policies only enforces the use of password with six characters. DirBuster did not find any interesting directories or files, scanning the website for vulnerabilities discovered nothing either. However since HTTP sends unencrypted traffic, it was possible to see information such as login credential in cleartext.

5.3.9 Case study IX

Description: Check for faulty SSL implementation in android application

Mallodroid's automatic scans did not reveal any inadequate SSL implementation or security issues for Arlo and Foscam.

Ring cam's application is implemented with TLS v.3 which is considered secure, but showed signs of one certificate with SHA1 hash.

5.3.10 Case study X

Description: Identify implemented encryption in the android application.

First of the ARM library files was investigated, by using string search it was established that all applications uses library functions that has to do with encryption and hash methods. Many hits for all devices on 'AES' and 'RSA', meaning they are likely used. An example of the command used to identify strings is shown in Figure 5.6.

The second part of the case was done by manually inspecting the code. In both Arlo and Foscam the use of Java Cryptographic Architecture was found which are cryptographic APIs and is found in the packages `java.security` and `javax.crypto`. Arlo also used `android.security.keystore` which is an API for storing and using keys [85]. Furthermore several classes having to do with encryption and encoding was found for Arlo as shown in Figure 5.5 which strengthen the previous findings of strings. In the Foscam application it was found on several places the use of encryption based on non-trusted packages as shown in Figure 5.7. The manual code review did not find anything of interest for the Ring application.

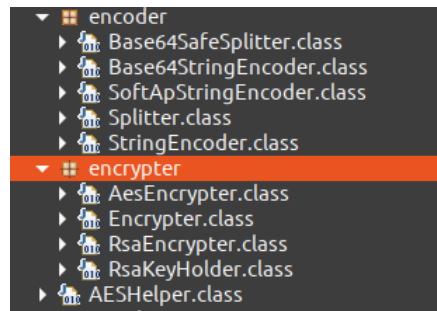


Figure 5.5: Arlo: Encryption and encoding classes

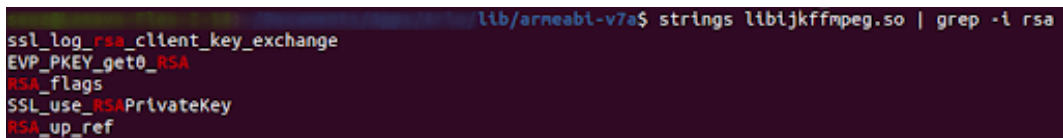


Figure 5.6: Command for identifying RSA strings

```
package com.foscam.myrsa;

public class MyRSA {
    static {
        try {
            System.loadLibrary("Rsa");
            return;
        } catch (Exception exception) {
            return;
        }
    }

    public static native byte[] encryptRSA(String paramString);
    public static native int loadRSAPublicKey(String paramString);
    public static native int unloadRSAPublicKey();
}
```

Figure 5.7: Foscam: Non-trusted encryption packages

5.3.11 Case study XI

Description: Verify privacy policies and settings in application.

Arlo and Foscam provided a link to the companies privacy policies, however no privacy settings or possibility to opt out of certain functionality was available. On the other hand, the Ring application provides the user with a control center where there is information about policies and the ability to modify settings for privacy and third party services shown in figure 5.8.

5.3.12 Case study XII

Description: Compare permissions in the android manifest and the features of the application to identify if the application is overprivileged.

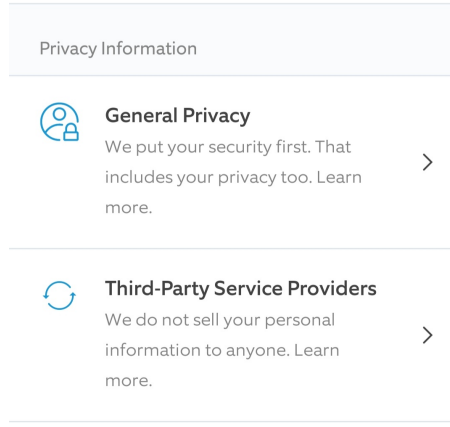


Figure 5.8: Ring Always Home: Offers the user ability to alter privacy settings

All devices require several permissions to function properly and in most cases they share the same permissions, a list of all permissions can be found under Appendix B. However none of the devices uses Bluetooth as a medium but all three applications have the permissions set to use Bluetooth. Although Arlo has other devices that supports the use of Bluetooth, the same can not be said about Foscam and Ring. None of the manuals or information available online shows the requirement for Bluetooth, even the Ring FAQ [86] states: *'No. Ring devices operate through wifi, not Bluetooth.'*

5.3.13 Case study XIII

Description: Use FlowDroid for taint analysis on the android application.

The tool FlowDroid was used for taint analysis and identifying possible data leaks. The Foscam device was by far the most talkative device with 156 reported leaks and also the device that talked with most external sources, 12 compared to Arlo(4) and Ring(5). In second place comes Ring with 52 reported leaks and last was Arlo with 11 reported leaks. In some cases sources of data was identified as e.g. `java.io.OutputStream` or `java.lang.String` which mean we can't see what type of data that is transmitted. However, Table 5.5 shows the instances of functions used where data could be identified.

<i>Arlo</i>	<i>Foscam</i>	<i>Ring</i>
getCountry()	getCountry()	No identifiable data
getSSID()	getSSID()	
getUserByExternalUserId()	getDeviceId()	
getLatitude()	getLatitude()	
getLongitude()	getLongitude()	
	getLastKnownLocation()	
	getSimSerialNumber()	
	getMacAddress()	
	getSubscriberId()	

Table 5.5: Identifiable data from the taint analysis

5.3.14 Case study XIV

Description: Perform a *Data Subject Access Request* to obtain a copy of data being processed on user.

The DSAR was sent on Mars 23 to all manufactures and every company responded within the first month. Arlo provided the data after six days, Foscam after two days and Ring provided the data after 19 days. The content for each response is presented one by one below:

Arlo

Arlo provided one pdf file containing the complete privacy notice, the email request and response of the DSAR and a copy of data undergoing processing. Data such as customer information, name, email address, country and address. In addition information about the device, information about support contact history and processed data with diagnostic tools. No information or further data about video streams or removed video content.

Foscam

Foscam provided three different categories of files. First a text file containing account information such as name, email address, gender, mobile phone, country, furthermore the file held information about the device. Second, a text file containing information on video alert captures with IDs, timestamps and alert category name. Third was a directory containing video files from motion alert captures. When the case study was conducted videos were captured on 19th of Mars with some of the videos being deleted from the cloud service, however the first capture received from the DSAR was dated, 21th of Mars.

Ring

/

```

├── app_events/
│   ├── 2021-03-15
│   │   └── ring_app.csv
│   ├── 2021-03-19
│   │   └── ring_app.csv
│   ├── 2021-03-22
│   │   └── ring_app.csv
│   ├── 2021-03-23
│   │   └── ring_app.csv
│   └── 2021-03-24
│       └── ring_app.csv
├── client_devices.csv
├── customer_support_messages.csv
├── devices.csv
├── events.csv
├── locations.csv
├── notification_client_devices.csv
├── other_events.csv
├── ring_neighbors/
│   ├── neighbors_alert_areas.csv
│   ├── neighbors_geosearch_alert_areas.csv
│   └── neighbors_users.csv
├── setups.csv
├── subscription_billing.csv
├── subscriptions.csv
├── user_linked_accounts.csv
└── users.csv

```

The tree is an overview of csv files that describes what information Ring has saved on the test user (author) designed for this case study. The *ring_app.csv* files contain performed activities for each day respectively, information about; "Setup", "Live Events", "Physical Installation", "Location Flow", "Tapped Tile", "Device Controls Menu", "Account Linking" and much more. Another interesting file is *users.csv* which consists of user details; email, name, phone number and created at. Live streams, photos and activity registered is stored to the cloud, however some data was removed:

- 2021-03-16 - ring_app.csv
- 2021-03-19 - ring_app.csv
- 2021-03-22 - ring_app.csv
- 2021-03-23 - ring_app.csv

Mentioned above was deleted prior to the DSAR but probably still remains on the cloud since that data was part of the DSAR response shows in the tree.

5.3.15 Privacy notice questions result

The Table 5.6 shows an overview of the summarised result from analysing the privacy notice behind each Camera provider. In the furthest left column is the question that is asked when reviewing the text, followed by the result found for each company. All three companies used a clear and understandable language and divided the privacy notice into relevant categories. However there was a noticeable difference in the amount of information presented and the level of transparency between the companies. In some cases information was missing for the questions asked. Important to notice is that the information in the table is a summary and some of the answers might have more detailed information in the policy, e.g. In the question "What personal data is collected?", all three companies had categories of collected personal data with many more specific details such as name, email, phone number and so on.

Table 5.6: Summarised result of reviewing the Privacay notice

Question	Arlo	Foscam	Ring
What personal data is collected?	Account info, order details access logs, device statistics	Account info, contact info, payment info, product setup info, device info, biometric info, social media handles, info processed on behalf of others	Account info, payment info, product setup info, technical info, third-party (social media, paypal,...), automated collection
When is personal data collected?	1) Register with website, landing pages or app. 2) Purchase a product or service. 3) Work with Arlo as a business partner.	Not mentioned	1) Using/interacting with products or services. 2) Register and use website, data usage and automated data.
What techniques are used to protect personal data?	1) TLS security. 2) Account authentication with secure login mechanism. 3) One-way hash functions with salt for all passwords. 4) Only store data for as long its needed.	1) Encryption technology and other means. 2) Limit range of peoples access to data, comply with confidentiality obligations. 3) Technical and physical safeguards to protect personal info. 4) Account info are systematic desensitisation	1) Administrative, technical and physical safeguards designed to protect personal info.
Continued on next page			

Table 5.6 – continued from previous page

Question	Arlo	Foscam	Ring
Which third parties are personal data shared with?	1) Government organisations and law enforcement. 2) Third parties: Banks, financial service providers, PR agencies, ..	1) We will not share or transfer your personal information to a third party. 2) In other circumstances consent will be obtained.	1) Affiliates and subsidiaries. 2) Our service providers, such as order fulfillment and data analytics.
What the data will be used for and how processing is limited to only what is necessary?	For each instance of different data that is processed it is clearly written what it is used for and how processing is done with references to the affected GDPR articles.	What the data is used for and how it is processed has it is own section and is illustrated in a clear way.	What the data is used for and how it is processed is clearly illustrated.
Is personal data collected “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”?	Only necessary data is stated to be collected for the purpose of processing.	Only necessary data is stated to be collected for the purpose of processing.	All data collected is claimed to be necessary, this because they also use data for customized advertising.
Continued on next page			

Table 5.6 – continued from previous page

Question	Arlo	Foscam	Ring
What is said about confidentiality and integrity?	1) Third parties have agreed to confidentiality restrictions and the use of personal data only for the contracted purpose. 2) We do not access your content without permission. 3) Personal information processed by cameras for alerts is done by AI and not human monitoring.	Limit the range of peoples access to data, comply with confidentiality obligations	Not mentioned
Is the data subject informed about their right to lodge a complaint with a supervisor authority against the controller?	Yes	No	No
Continued on next page			

Table 5.6 – continued from previous page

Question	Arlo	Foscam	Ring
When data is transferred to a country outside EU or an international organisation, is the data subject informed of the safeguards put in place relating to this transfer?	Yes: 1) Transfers within Verisure Group, agreement that ensures adequate and consistent level of protection. 2) Assurances covered by certificate such as EU US Privacy shield. 3) Requests from law enforcement is carefully validated before personal data is shared. 4) You have the right to contact us about more info about safeguards.	Not clearly: When personal info is transferred to the US, we will take measures to protect that info.	Yes, to some extent: Mentions the use of EU-US Privacy Shield principles but also writes; When personal info is transferred to other countries such as the US, adequate protection for transfer is provided.
Is the data subject informed about their right to “request if their information is rectified, removed or that its processing is restricted by the controller”?	Yes	Yes	Yes
Is the data subject informed about their right to “object to data processing”?	Yes	Yes	Yes
Continued on next page			

Table 5.6 – continued from previous page

Question	Arlo	Foscam	Ring
Is the information provided “In a concise, transparent, intelligible and easily accessible form, using clear and plain language”?	Yes: The language is clear and easy to understand, the info is categorized in relevant sections and with multiple references to the corresponding GDPR articles it covers.	Yes, to some extent: Clear and understandable language divided into categorises, Some info is not clearly presented in a transparent way. Not as thorough info	Yes: Clear and easy to understand, categorized sections and adequate info.

Chapter 6

Analysis and Discussion

This chapter starts by explaining the projects limitations and then analysing the results from previous phase and discusses findings and how it was interpreted.

6.1 Research limitations

The major restraint for the case studies were due to not being capable of decrypting the network TLS transmission. TLS is a recommended security standard that provides traffic encryption to ensure reliability when devices interact. However, this led to some case studies not providing a complete conclusion of the matter. With the authors experience and knowledge, Arlo cam and Ring cam's encryption implementation could not be manipulated. Therefore, it is impossible to be certain of how they handle the encrypted data between the device and cloud or device and smart phone.

Because the methodology was not necessary individually designed for each camera and more of a generic IoT camera methodology, some methods worked better on some cameras and vice versa. The amount and success of extracting information depended on how the device or application was structurally built. This determines the outcome of the results and has a significant impact on the thesis.

The amount of code to go through manually for the three applications was enormous and reviewing the entire code by hands would take weeks, which was not possible with the time constraint. The use of automated tools was used to aid in some areas, however because lack of knowledge there might be certain techniques and tools missed by the authors.

None of the cameras was equipped with physical ports apart from micro USB as a power source. This declined the physical Category for our tests, however the they still remain in the thesis to demonstrate our awareness of those issues.

Many assumptions in discussion and findings in result is based on the android application, the outcome would most likely differ for other platforms.

Because there were three selected devices, the distribution of time restricted a detailed examination for each camera. For this project's timetable, one or two devices would be preferred for a deeper and more fulfilling analysis.

6.2 Case study analysis and discussion

This section analyses and discusses all case study separately for each camera and provides a summary of the privacy notice analysis.

6.2.1 Case study I

Because of the complexity to decrypt TLS, and all cameras were implemented with it, only DNS could be properly investigated. The cameras only seemed to communicate with servers of their own domain respectively. They share similar connections to sub-domains seemingly for various purposes, like firmware update, data storage and API:s. Similarly they all are associated with a different third party NTP server.

No sign of any suspicious DNS requests that could lead to unknown endpoints or point to illegal data sharing to distinctive remote servers. However, as previously mentioned this is only based on the DNS connections because the traffic is encrypted. TLS encryption is automatically activated and signifies proper security which fulfils the tested principles.

6.2.2 Case study II & III

Identically to Case study I, the traffic was encrypted which only allowed for connectivity observing. The devices communicate with several different IP addresses, but what is interesting is how the majority of the connections suggest to vary depending on the company. All cameras seem to have a partnership with Amazon or at least running their storage servers on Amazon's cloud service. Amazon is a huge company with various functionality for cloud services which allows IoT devices to simply connect to the constructed infrastructure.

While interacting with the cameras in various ways, the traffic was carefully monitored to ensure what interaction generated what behaviour. When streaming live video or uploading the motion detection picture, Arlo and Ring, as expected, stored the data on a EU server. Whereas normal activity like customising settings was transmitted to servers located in USA, possibly because of availability of servers and lower costs. Foscam stored user data on servers placed in USA but clarified this in the privacy notice which is approved by GDPR.

This entails that the devices comply with GDPR in this circumstance by not storing sensitive data on servers outside EU without informing the user. Obviously the tests are limited to our network structure, the data that transfers after it has arrived to the devices' servers are outside the scope.

6.2.3 Case study IV

The nmap scans did not reveal any open ports for Arlo or Ring, those cameras are directly connected to cloud servers and does not run services locally. However, Foscam runs a few services locally; `lighttpd`, `https`, `gsoap`, `rtsp` and one unknown service. The structure of Arlo and Ring suggests that greater security is taken in consideration since local services often comes with additional risks. Though this force users to have their devices connected to the internet for their cameras to work.

It also helps prevent attacks when a malicious user has invaded the network because there are no local ports exposed for intrusion on the devices. Although Foscam might have ports open, the services running are implemented with security measures which increases overall security, yet not to the extent as of avoiding open ports at all. Also having an unknown port open is not very transparent and might lead to unknown security implications.

Contrarily, if the servers continuously communicating with the cameras would be infected with malware or jeopardised. That would potentially allow the attacker to breach the cameras as well which could lead to privacy concerns.

By disregarding open ports and running service locally a safer environment is created for the average user, rather than having possible exploitable ports open. PbD principle 2 requires the manufacturer to assure secure systems without user interaction. Another infrastructure for Foscam could possibly improve the protection against attacks, on the other hand, the open ports are implemented with security.

6.2.4 Case study V

Because Foscam does not verify non-trusted certificates, an attacker, under some circumstances could observe network traffic in plain text. The visible content, contains of motion detection photos, websites, secret-keys and MAC addresses. This allows an eavesdropping user to recreate the raw image data into the original figure. This raises privacy concerns since motion detection pictures are often generated from people's movement. Depending on the situation of when the photo is taken, a person's face could be transferred over an insecure network, which obviously is highly sensitive data. Identifiable information requires careful data management to not expose users without intent.

Other data such as the URI:s seemed to be protected with SSL pinning, when modifying the packet to a malicious website, the system responded with errors. The example in figure 5.3 demonstrates what the captured motion detection photo appears like in *ZAP*.

The Arlo and Ring cam both restricts certificates that does not origin from a trusted source. This denies the possibility to abuse the cameras transmission between them and their cloud service.

This is a serious vulnerability which should be investigated by the company. This indicates that Foscam can not ensure protected end-to-end communication, therefore, failing to satisfy PbD principle 5.

6.2.5 Case study VI

The presented FCC ID on the physical devices of Foscam and Ring is no necessary sensitive information. However it provides a user with detailed knowledge about the hardware of the device. It is highly unlikely that the exposure of FCC ID alone would cause malicious attacks, but it is an interesting feature that probably could be handled differently. Arlo keeps this data hidden under the device information of the application, which is potentially a safer way of storing FCC ID.

Foscam offers the freedom to store video streams and photos locally straight to a removable SD card. Unfortunately, lack of time and no access to SD cards prevented

further examination of the transmission between the camera and the memory card. However, if the data would be stored unencrypted or could be monitored by an attacker in some way, there is a great risk of privacy concern. In that case, if someone would acquire the SD card physically that person would have access to all unencrypted and possibly sensitive data.

6.2.6 Case study VII

Ignoring gearing the devices with serial ports increases the security because oftentimes the capability of connecting wires includes vulnerabilities.

6.2.7 Case study VIII

Foscam somewhat overlooks the importance of password policies in the web application, it only requires the user to select a password of six characters which can be brute-forced instantly. The device is not developed with security measures against brute-force attacks which together with previous example produces a vulnerability once an attacker has gained local access. The local unencrypted traffic also allows users to eavesdrop on login credentials, if someone were to gain access to the device they could operate the camera in any way desired.

Foscam can not meet the requirements for PbD 5 since sensitive data can be accessed once an attacker has breached the network. Security by default would most likely anticipate that the system forces users passwords longer than six characters and containing letters, numbers and symbols.

6.2.8 Case study IX

Mallodroid illustrated that SSL was implemented without any faulty alerts. The Ring device showed signs SHA1 hashes for one certificate. SHA1 hashes is considered to be obsolete and should not sign certificates, this could lead to bypassing the SSL encryption. However, from this tool alone it was impossible to resolve where the certificate was operating. Analysing the source code for the application would be too excessive for this paper, which prevented the case study to continue.

Considering the ambiguity of how the SHA1 hash was utilised, it is problematic to assume the outcome of exploiting the potential vulnerability. Needless to say, the PbD principles affected can not be answered.

6.2.9 Case study X

Identifying the encryption for the application contributes to the penetration process for an attacker. The findings for this case study mostly refers to AES and RSA encryption methods. They are both typical and reliable approaches used for a great deal of scenarios. Reverse engineering how the encryption methods operate, may help determine how to decrypt the data. However, the uncertainty of the information's origin complicates revealing the encryption process. Since the results does not clarify exactly where, what or how the methods function, no decision of its security level can be established. Also, the version of encryption or key length could not be

determined, which would have strengthened the knowledge if best practice was followed for cryptography. The code review of the Arlo application was the only one identified to clearly follow guidelines of the OWASP android testing guide[74] or a similar guideline, with the use of cryptographic APIs and proper implementation for storing and using cipher keys. This might be true for the other applications but could not be verified by manual code review.

6.2.10 Case study XI

Ring Always Home application provides the opportunity to adjust settings regarding general privacy and third-party options. Arlo and Foscam presents a link to respective companies privacy policies but disregards the option to alter settings. Like previously mentioned, [48] explains how corporations often implements comprehensive privacy notice and policy utility with alternatives or almost overlooks privacy concerns completely. This could indicate that companies are either completely aware or unaware of the importance of GDPR's recommendations.

Because all applications, provide or links to, privacy policies the PbD principle 6 is satisfied. An improvement for Arlo and Foscam would be to include privacy settings within the application.

6.2.11 Case study XII

Several permissions granted by the mobile application is necessary for the functionality of the application, such as access to external storage, WiFi information, internet connections and alerts. The most interesting finding is the permission for the use of Bluetooth, specifically for Ring and Foscam since no information about the use of Bluetooth was found in for their products. Foremost Ring explicit mentions in their FAQs that they do not use Bluetooth for their devices. As well as being the only application using the permission *Bluetooth_privileged* which allows pairing of Bluetooth devices without user interaction. An argument can be made that the two application are overprivileged. It could also be possible that older versions of Ring cameras has offered Bluetooth as a setup technology but is no longer in use, then the application should be updated accordingly. Generally from a security and privacy standpoint, applications should not request permissions that is not essential for its goal. It generates unnecessary possible vulnerabilities and if it requests more than crucial, it should be stated why. Also all applications has the permissions to collect the users location, perhaps the user location is not necessarily needed for an application controlling a camera. But both Arlo and Ring mentions the collection of location data in their privacy policies. On the contrarily Foscam does not mention the collection of location data in their privacy policy, which is disagreeable considering PbD principle 6: Visibility and transparency.

6.2.12 Case study XIII

The results illustrate that the Foscam application implementation leaks a remarkable amount of data compared to the others with 156 leaks to 52 and 11 for Ring and Arlo correspondingly. However it is important to notice that some reported leaks

can be a necessity for the functionality of the application and not necessarily a bad thing, but the amount of data leaked and to a bigger number of outside entities shows poorly on confidentiality and integrity. Arlo's low number suggests that more security has been taken into consideration while designing the application in contrast to the others. PbD proclaims the significance of including security in the process of implementing systems. However, the size and complexity of the application also plays a part when designing a secure system.

- Foscam - 56 MB
- Arlo - 82 MB
- Ring - 124 MB

Some would assume a larger application generates additional vulnerabilities because it presumably contains more functions to exploit. It could also be argued that a limited application has not implemented enough security measures. Analysing these three applications' volume, the size is supposedly not the major factor of the security, rather the content's implementation.

These leaks implies unsatisfactory usage of built-in functions or inputs that could be exploited. Analysing every single leak for each camera would demand exploring the source code for each application and find possible exploits. That would be too excessive for this thesis, therefore, presenting this result functions as an alert of possible security holes.

Depending on the vulnerabilities and possible exploits discovered out of these leaks, different PbD principles could have been affected.

6.2.13 Case study XIV

First of, all companies delivered the DSAR response within the specified time frame. An email was sent to each manufacturer requesting the DSAR, Ring replied instantly with their privacy notice information and a link to where the request could be processed. About ten minutes later a confirmation mail described that the application progress would take less than 30 days and a notification would be sent once the data is available. The DSAR progress was reasonable and provided a substantial amount of information, however, some data still remained after deletion. This could be an indicator that the data is still stored on the cloud server after it was removed. On the other hand, it is likely the erasure takes a few moments before actually being deleted. Which in this case, would allow the DSAR to be performed prior to the data removal to occur.

Arlo's manufacturer delivered all registered user information and some device data generated from their diagnostic tool, but the least amount of general data. Based on Arlo's notable performance from the tests and its GDPR awareness, it is reasonable that the company stores a smaller amount of data compared to the other two, rather than withholding information saved to their servers. Then again, no further information about video streams, removed data or motion alerts was provided. Both Foscam and Ring delivered information about video history and alerts. The Ring response distributed the most information about the data collected

which indicates good transparency. Foscam was very quick to respond and delivered the DSAR in a downloadable form from their website, which indicates that they have set up a system to handle DSAR requests.

6.2.14 Privacy notice analysis

The first thing to mention is that neither of the authors have a background within jurisprudence, meaning that interpretation of legislation's comes from a limited knowledge. All three companies are very thorough when it comes to what type of data they process and what the purpose is behind the processing. Likewise all companies have presented the personal data in relevant categories. When data is collected might not be a strictly applicable requirement but it shows that the company is transparent, this was done by Arlo and Ring but not by Foscam. Arlo and Ring meticulously write about the legal basis for the use of personal information which is a requirement of the GDPR (Article 13.1.c). Both companies have their own section for this and specially Arlo is being very accurate with references to the GDPR legal basis on every section regarding a new type of data processing. On the contrary Foscam is probably lacking a bit with this information as the only information available about legal basis is the statement *"Comply with and enforce applicable legal requirements"*. Another requirement of the GDPR (Article 13.2.d) is to inform the data subject about *"the right to lodge a complaint with a supervisory authority"*, this was missing for both Ring and Foscam.

There is a significant difference when information is presented between all three companies but foremost between Arlo and Ring compared to Foscam. E.g. Foscam: *"we will use encryption technology and other means to protect your personal information"*, what kind of encryption is not stated and the phrase "other means" can mean a lot of things. On the other hand Arlo specifically writes about technologies used such as TLS and one-way hashes, as well as other counter-measures to protect personal data. In the end, all companies have covered the most fundamental information about the data processing they do in their privacy policies. Arlo is delivering the most amount of information and being most transparent. Both Ring and Foscam had some information missing which was requirements of GDPR. Although Ring delivers more transparent information than Foscam which had by far the least amount of text in their policy. However there are studies [48, 49] that have concluded that many people do not read companies policies because they are long and complicated. Therefore having the most specific and long text might not be the best solution.

6.3 Discussion of case study and findings

The purpose of this thesis was to evaluate three different cameras' characteristics and compare the results to how well it complies with GDPR legislation and the Privacy by Design principles 2, 5 & 6. This was accomplished by constructing several tests designed to research security flaws and improper handling of sensitive data, in a virtual environment. The tests were formed by the authors with the supervisors approval to support answer the research questions.

Collecting the result and discussion of each case study, the evidence suggests

that the Arlo cam may perhaps be the safest implemented camera from the PbD standpoint out of the three. Its case study performance implies that careful security and data management has been taken into consideration from the beginning of the development progress. It is not unreasonable to assume a framework for development has been utilised to comply with GDPR.

In the past, Ring has suffered some lawsuits [61] as a consequence of various unpleasant hacks which labelled Ring with poor reputation in some communities. The popularity and privacy concerns of this device made it an attractive camera for research purpose. What was interesting to see is that several previously known vulnerabilities has been patched and various additional improvements has been implemented. Which suggests that Ring is actively enhancing its products for the better and stays updated with the industry.

According to the presented results, Foscam showed the least satisfying privacy protection. Its infrastructure differed to the other cameras and could be one reason for its lack of security measures. Running servers locally contributed to a few vulnerabilities, forcing "camera to cloud" technology could possibly benefit the system's infrastructure and security.

In general, the implemented security in all cameras exceeded the expectations based on previous related work and articles from past years. This indicates that the industry improves in the security aspect over time and companies recognises the importance of implementing reliable protection measures for IoT devices. The actual level of protection could possibly rely on the device expense, presumably a costly camera is more likely to afford state of the art technology and security. The manufacturers were also well aware of the GDPR's *Data Subject Access Request* which must be available for all data-storing devices.

6.3.1 Research Question 1

What type of data is stored on the selected IoT smart cameras, how is the data managed and what countermeasures are implemented to protect the privacy of the user?

case study 1 & 2 demonstrated that the communication from all devices to internet is encrypted with TLS which is a legitimate and useful method of protecting data transmissions. Arlo and Ring have a similar structure where the devices are required to connect to the internet before operating, to download latest firmware to ensure an updated and patched software. Also, all communication from the devices passes through internet to their cloud services, which prevents any local attacks. The tests also reveal that no data seem to be stored locally or at some unexpected server, all transmissions are delivered to reliable and legitimate servers.

Foscam on the other hand, runs a local HTTP webserver which transports unencrypted traffic on port 80, which not only limits the security measures but also signifies sensitive data in clear text for eavesdropping in the network. HTTP was used on the internal network for the control and access to the camera stream and therefore share no PII except the video stream. However external communication is transmitted to the cloud over secure communication. The RTSP service of the Foscam device uses proper authentication to avoid unauthorised access. Also all systems identified cloud communications used appropriate authentication.

6.3.2 Research Question 2

to what extent are the Privacy by Design principles applied to application and design? What can be improved?

Based on the results, the Arlo camera and application shows signs of ensuing a framework like *Privacy by Design* or similar. None of the test uncovered concrete validation of data misuse or poor security standards. However, Case study XIII reported 11 potential leaks on the application. Although as mentioned, it is unclear what type of leaks and what impact they could have on the application since it was not evaluated in this thesis. One suggestion closely related to visibility and transparency is to implement privacy settings in the application, which provides users the ability to opt out of certain functionality. This is not a requirement by GDPR but is encouraged.

The result implies that Ring adheres to GDPR regulations and possibly adopted a framework while designing and implementing the device and application. Nearly none of the test raised any critical flags for Ring, however there are some minor findings that should be elevated. Ring Always Home seems to request more permission than necessary for its purpose, Bluetooth permission is required but there is no Bluetooth functionality. PbD principle 6 demands that companies are transparent with the data usage and intentions, removing or describing the Bluetooth permission could increase their credibility. The taint analysis from Case study XIII announced 52 leaks, but similarly to the Arlo, the impact has not been investigated. The *Data Subject Access Request* process was practical and effortless, the result however revealed that removed data still remained on their servers. Although the privacy policy was well written it could benefit from more precise explanation on what tools and techniques are used to protect user privacy.

Based on the tests, most likely Foscam's infrastructure and application does not currently adhere to a framework to meet the GDPR requirements to its full extent. It suffers from a few vulnerabilities and would presumably benefit from incorporating a framework like PbD. It might be necessary to reconstruct the foundation of the system, not running local servers and adjusting the certificate handling is unavoidable. There are also fundamental flaws in the information provided in the privacy policies that should be addressed to comply with GDPR and adhere to PbD principle 6, visibility and transparency. Also being the most talkative application with 156 leaks to external sources and being the smallest application reflects poorly on transparency, integrity and confidentiality.

6.3.3 Research Question 3

How does the current data regulation laws (GDPR) impact or should impact IoT device design and operation?

To comply with GDPR, manufacturers are required to make an effort to increase security standards in IoT devices. By integrating a framework that guides the development to an approved, official and established standard. IoT devices would probably improve its overall security but more specifically privacy and data management. The

privacy policies of all companies discuss the use of security standards and techniques to comply with GDPR, therefore GDPR probably have had an impact in the design and operation of IoT systems. However there was a noticeable difference in the security implementations and also how transparent each company is. The GDPR should perhaps have references to recommended security standards and framework for different areas affecting the IoT spectrum such as the OWASP android security guide or frameworks for creating privacy policies and so on. This could simplify complying with GDPR and strengthen the overall security of IoT systems in general.

Chapter 7

Conclusions and Future Work

This thesis shows how different IoT systems handles processing of data. What type of data the systems stored was partially identified through network analysis, static analysis and a DSAR request. However because the systems all used encryption methods, all processed data could not be evaluated. It can be said that all companies have taken GDPR and the selected PbD principles into consideration when developing their systems. Security and privacy was considered as all systems was identified to use standardised encryption methods, TLS, AES and RSA. Proper authentication methods was used to avoid unauthorised access. Data life-cycle protection was considered since all companies mentioned where data was transferred which matched the research performed on communications with IP-addresses, although it was not possible to analyse communications made after data was transmitted to the cloud service. Visibility and transparency was considered as all companies provided the DSAR request within reasonable amount of time and they had reasoned what/how/why personal data may be processed in their privacy policies. However to what extent the companies had followed GDPR and PbD, there is a noticeable difference.

The biggest security issues were found in the Foscam system which did not verify the certificate for the TLS service meaning some encrypted traffic was seen in clear text. Despite the fact that no PII was delivered, other sensitive data such as the device MAC address and a raw-image of the camera capture was transmitted, which could include visuals of individuals. Other smaller issues was using HTTP service with poor security mechanisms and having unknown or unnecessary ports open. In the Ring android application an outdated hash method SHA1 was identified but the system had no other significant security issues. The Arlo system had no identified security issues at all.

Another area researched was how transparent each company is with the data being processed. Reviewing the privacy policies it was noted that Arlo was by far the best at providing transparent information and missed no requirements, on the contrary both Ring and Foscam failed to meet GDPR requirements in some aspects. However Ring is much more transparent and provides more valuable information than Foscam. As for example, the taint analysis on the android application identified that Foscam and Arlo collected the location of the user. However only Ring and Arlo mentioned the collection of user location in their privacy policy, not Foscam. The taint analysis also showcased that Foscam by far sent data to outgoing sources despite being the smallest application with the least functionality. By the information provided by the DSAR request, all companies adhere to the GDPR requirements but the Ring showed most transparency with sending the most data. Ring was also the only company

providing the possibility to alter privacy settings, which is a tool all companies that collect sensitive data should provide.

It is important for the consumer to take part in reading the privacy policies and terms and conditions of IoT manufactures, so they understand how their personal data is used and can make an informed decision before buying a product. Furthermore opting to buy a product which heavily focus and markets their security technologies such as Arlo may not be the right choice for every consumer. There are other options that have good security and privacy solutions and in the end it is the consumers responsibility to be aware of security and privacy when buying products.

Despite the difference in the result between the devices, looking at all the security and privacy mechanisms discussed in this thesis and with all policies mentioning GDPR it is safe to say that data regulations have had a strong impact for the better on these IoT systems. Another motivation for this conclusion is the fact that both Ring and Foscam had multiple older reported security and privacy issues, which was reviewed when selecting the devices and they seem to have implemented better security standards since then. There are traces of the PbD principles in all selected systems but foremost in Arlo and Ring, Foscam could benefit from reviewing and working more with the concept of PbD.

7.1 Future work

There are many possibilities for future studies in the area researched by this thesis. One approach is to apply this methodology to either research a greater amount of IoT cameras or research a completely new field of IoT devices, for example, wearable-IoT devices. Furthermore the case study can be changed to target other principles of the PbD concept and use more extensive methods. For example the taint analysis and other static analysis methods have been described as a useful tool to investigate GDPR compliance and find vulnerabilities [27, 40]. This method was very limited in this paper and further research can be made.

Another approach could be to have more focus on IoT applications. Because of time constraints, the methodology was limited to manual code review and static analysis, there are however methods for dynamic analysis for security and privacy auditing. Because the project was limited to android applications, future research can be extended to iOS applications. Also the study [52] describes methods to circumvent SSL pinning on IoT android applications in order to see encrypted traffic in clear text. This can then be examined to analyse how sensitive data is processed in correlation with GDPR and PbD.

An additional area would be to investigate privacy policies of IoT manufacturers, there was a distinct difference in the amount and type of information shared in the three policies investigated. Future research could focus on a wider selection of privacy policies to identify weaknesses and problems with how companies interprets the GDPR and potential solutions.

Bibliography

- [1] State of the iot 2020: 12 billion iot connections. [Online] Available at: <https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/>. [Accessed: 04-Jan-2021].
- [2] Ericsson: The internet of things (iot) technology. [Online] Available at: <https://www.ericsson.com/en/internet-of-things/iot-security>. [Accessed: 04-Jan-2021].
- [3] Kaspersky: Internet of things security threats. [Online] Available at: <https://www.kaspersky.com/resource-center/threats/internet-of-things-security-risks>. [Accessed: 04-Jan-2021].
- [4] D. Strom. Return of mirai botnet. [Online] Available at: <https://blog.avast.com/return-of-mirai-botnet-avast>. [Accessed: 21-Jan-2021].
- [5] Avast Threat Intelligence Team. New torii botnet uncovered, more sophisticated than mirai. [Online] Available at: <https://blog.avast.com/new-torii-botnet-threat-research>. [Accessed: 21-Jan-2021].
- [6] B. Nelson. This is the most vulnerable smart device in your home right now. [Online] Available at: <https://www.rd.com/article/most-vulnerable-home-smart-device/>. [Accessed: 12-Sep-2019].
- [7] General data protection regulation. Official J. Eur. Union, vol.59 L119, pp. 1–90. [Published: 04-May-2016].
- [8] R. Alharbi and D. Aspinall. An iot analysis framework: An investigation of iot smart cameras' vulnerabilities. 2018. DOI: 10.1049/cp.2018.0047.
- [9] P. A. Abdalla and C. Varol. Testing iot security: The case study of an ip camera. *8th International Symposium on Digital Forensics and Security (ISDFS)*, 2020. DOI: 10.1109/ISDFS49300.2020.9116392.
- [10] J. Liranzo and T. Hayajneh. Security and privacy issues affecting cloud-based ip camera. *IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference*, 2017. DOI: 10.1109/UEMCON.2017.8249043.
- [11] A. Manske. Conducting a vulnerability assessment of an ip camera. *DEGREE PROJECT IN COMPUTER SCIENCE AND ENGINEERING, KTH*, 2019.
- [12] S. Wachter. Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the gdpr. *computer law security review 34 (2018) 436–449*, 2018.
- [13] A.D. Kounoudes and G.M. Kapitsaki. A mapping of iot user-centric privacy preserving approaches to the gdpr. *Internet of Things Volume 11, 100179*, 2020.

- [14] C. Li and B. Palanisamy. Privacy in internet of things: From principles to technologies. *IEEE INTERNET OF THINGS JOURNAL*, VOL. 6, NO. 1, 2019.
- [15] B. Alamri, I. Javed, and T. Margaria. Preserving patients' privacy in medical iot using blockchain. in *Edge Computing – EDGE 2020*, Cham: Springer International Publishing, page 103–110, 2020.
- [16] R. Lomotey, K. Sofranko, and R. Orji. Enhancing privacy in wearable iot through a provenance architecture. *Multimodal Technologies and Interaction*, page 18, 2018.
- [17] Samuel D. Warren and Louis Brandeis. *The right to privacy*. 1890.
- [18] Allan Westin and Bloom-Cooper Louis. *Privacy and freedom*. 1970.
- [19] Jaap-Henk Hoepman. Privacy design strategies. *IFIP Advances in Information and Communication Technology*, 2014.
- [20] United Nations. Universal declaration of human rights. [Online] Available at: <https://www.un.org/en/universal-declaration-human-rights/>. [Accesed: 02-Mar-2021].
- [21] Eu directive 95/46/ec. [Online] Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046>. [Accesed: 02-Mar-2021].
- [22] IT Governance Privacy Team. *EU General Data Protection Regulation (GDPR) - an Implementation and Compliance Guide*. I. T. Governance, 2020.
- [23] Information Registratiekamer and Privacy Commissioner/Ontario. Privacy-enhancing technologies: the path to anonymity. *Achtergrondstudies en Verkenningen 5B, vols. I and II*, Rijswijk, 1995.
- [24] A. Cavoukian. Privacy by design - the 7 foundational principles. *Information and Privacy Commissioner of Ontario*, 2009.
- [25] B. Russell. Fundamentals of iot security. [Online] Available at: <https://learning.oreilly.com/videos/fundamentals-of-iot/9781788392075>. [Published: 2017].
- [26] W.M. Kang, S.Y. Moon, and J.H. Park. An enhanced security framework for home appliances in smart home. *Human-centric Computing and Information Sciences*, 2017.
- [27] P. Ferrara, A.K. Mandal, A. Cortesi, and F. Spoto. Static analysis for discovering iot vulnerabilities. *International Journal on Software Tools for Technology Transfer (2021)* 23:71–88, 2020. DOI: <https://doi.org/10.1007/s10009-020-00592-x>.
- [28] K. Loukil, M. Khalfa, M. Wassim Jmal, T. Frikha, and M. Abid. Design and test of smart ip-camera within reconfigurable platform. pages 25–29, 2017. DOI: 10.1109/Anti-Cybercrime.2017.7905257.
- [29] J. Bugeja, D. Jönsson, and A. Jacobsson. An investigation of vulnerabilities in smart connected cameras. pages 537–542, 2018. DOI: 10.1109/PER-COMW.2018.8480184.
- [30] A. Gupta. *Performing an IoT Pentest. The IoT Hacker's Handbook*, 17–37.

2019. DOI: 10.1007/978-1-4842-4300-8_2.

- [31] B. Dinis and C. Serrao. External footprinting security assessments. *International Conference on Information Society (i-Society 2014)*, 2014.
- [32] Kurose James F and Ross Keith W. *Computer networking: a top-down approach (7th, Global ed.)*. Harlow: Pearson Education, 2017.
- [33] Man page of tcpdump. [Online] Available at: <https://www.tcpdump.org/manpages/tcpdump.1.html>. [Accessed: 2021-04-13].
- [34] Wireshark user guide. [Online] Available at: https://www.wireshark.org/docs/wsug_html_chunked/. [Accessed : 2021 – 04 – 13].
- [35] C. Gibler, J. Crussell, J. Erickson, and H. Chen. Androidleaks: Automatically detecting potential privacy leaks in android applications on a large scale. *Trust and Trustworthy Computing, 2012*, 2012.
- [36] Guide to app architecture. [Online] Available at: <https://developer.android.com/jetpack/guide>. [Accessed: 2021-04-14].
- [37] Z. Berkay Celik, P. McDaniel, G. Tan, L. Babun, and A. Selcuk Uluagac. Verifying internet of things safety and security in physical spaces. *IEEE Security Privacy, vol. 17, (5), pp. 30-37*, 2019. DOI: 10.1109/MSEC.2019.2911511.
- [38] E. Fernandes, J. Paupore, A. Rahmati, D. Simionato, M. Conti, and A. Prakash. Flowfence: Practical data protection for emerging iot application frameworks. *25th USENIX Security Symposium*, 2016.
- [39] A. Acar, H. Fereidooni, T. Abera, A.K. Sikder, M. Miettinen, H. Aksu, M. Conti, A. Sadeghi, and S. Uluagac. Peek-a-boo: I see your smart home activities, even encrypted! *13th ACM Conference on security and privacy in wireless and mobile networks*, 2020. DOI: 10.1145/3395351.3399421.
- [40] P. Ferrara and F. Spoto. Static analysis for gdpr compliance. *Proceedings of the 2nd Italian Conference on Cybersecurity (ITASEC)*, 2018.
- [41] Http over tls. [Online] Available at: <https://tools.ietf.org/html/rfc2818>. [Accessed: 2021-04-22].
- [42] Certificate authority (ca). [Online] Available at: <https://www.techopedia.com/definition/29742/certificate-authority-ca>. [Accessed: 2021-04-29].
- [43] S. Wachter. The gdpr and the internet of things: a three-step transparency model. *Law, Innovation and Technology, 10:2, 266-294*, 2018. DOI: <https://doi.org/10.1080/17579961.2018.1527479>.
- [44] D. Bastos, F. Giubilo, M. Shackelton, and F. El-Mousa. Gdpr privacy implications for the internet of things. *4th Annual IoT Security Foundation Conference*, 2018.
- [45] M. BARATI, O. RANA, I. PETRI, and G. THEODORAKOPOULOS. Gdpr compliance verification in internet of things. *IEEE Access, vol. 8, pp. 119697-119709*, 2020.
- [46] A. Chaudhuri and A. Caoukian. The proactive and preventive privacy (3p) framework

for iot privacy by design. *EDPACS, 01/2018, Volume 57, Issue 1*, 2018.

- [47] S. Page and K. Rannenbergh. Applying privacy patterns to the internet of things' (iot) architecture. *Mobile Networks and Applications*, vol. 24, (3), pages 925–933, 2019.
- [48] P. Shayegh and S. Ghanavati. Toward an approach to privacy notices in iot. *2017 IEEE 25th International Requirements Engineering Conference Workshops*, 2017.
- [49] K Renaud and L.A. Shepherd. How to make privacy policies both gdpr-compliant and usable. 2018. DOI: DOI: 10.1109/CyberSA.2018.8551442.
- [50] A. Tekeoglu and A.S. Tosun. A testbed for security and privacy analysis of iot devices. *2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems*, 2016.
- [51] Y. Seralathan, T. (Tom) Oh, S. Jadhav, J. Myers, J. (Paul) Jeong, Y. Ho Kim, and J. Noyo Kim. Iot security vulnerability: A case study of a web camera. *International Conference on Advanced Communications Technology(ICACT)*, 2018.
- [52] A. Subahi and G. Theodorakopoulos. Detecting iot user behavior and sensitive information in encrypted iot-app traffic. *Sensors (Basel, Switzerland)*, vol. 19, (21), pp. 4777, 2019.
- [53] K. Knorr and D. Aspinall. Security testing for android mhealth apps. *IEEE Eighth International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, 2015.
- [54] S. Arzt, S. Rasthofer, C. Fritz, E. Bodden, A. Bartel, J. Klein, Y. Le Traon, D. Octeau, and P. McDaniel. Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps. 2014. DOI: 10.1145/2594291.2594299.
- [55] B. Kitchenham and S. Charters. Guidelines for performing systematic literature reviews in software engineering. *Keele University and Durham University Joint Report*, 2007.
- [56] NETGEAR. Netgear® announces planned separation of its arlo business. [Online] Available at: <https://investor.netgear.com/releases/press-release-details/2018/NETGEAR-Announces-Planned-Separation-of-its-Arlo-Business/default.aspx>. [Accessed: 01-Feb-2021].
- [57] F-secure. Vulnerabilities in foscaml ip cameras. [Online] Available at: https://blog.f-secure.com/wp-content/uploads/2017/06/vulnerabilities-in-foscaml-ip-cameras_report.pdf. [Accessed : 2021 – 02 – 3].
- [58] O. Peles. Major vulnerabilities and exploit in foscaml cameras. [Online] Available at: <https://www.vdoo.com/blog/vdoo-has-found-major-vulnerabilities-in-foscaml-cameras>. [Accessed: 2021-02-03].
- [59] A. Montag and S. Berger. Amazon bought 'shark tank' reject ring last year—here's what the founder says about jeff bezos. [Online] Available at: <https://www.cnbc.com/2018/02/27/amazon-buys-ring-a-former-shark-tank-reject.html>. [Accessed: 01-Feb-2021].
- [60] B. Budington. Ring doorbell app packed with third-party trackers. [Online] Available at: <https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party>

- trackers. [Accessed: 01-Feb-2021].
- [61] Dozens sue amazon's ring after camera hack leads to threats and racial slurs. [Online] Available at: <https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats>. [Accessed: 2021-05-04].
 - [62] dnsmasq. [Online] Available at: <https://wiki.debian.org/dnsmasq>. [Accessed: 2021-04-14].
 - [63] whois manual page. [Online] Available at: <https://tools.ietf.org/html/rfc3912>. [Accessed: 2021-04-20].
 - [64] nslookup manual page. [Online] Available at: [https://man.cx/nslookup\(1\)](https://man.cx/nslookup(1)). [Accessed: 2021-04-20].
 - [65] Ip location. [Online] Available at: <https://www.iplocation.net/ip-lookup>. [Accessed: 2021-04-16].
 - [66] Searchable fcc id database. [Online] Available at: <https://fccid.io/>. [Accessed: 2021-04-20].
 - [67] Nmap security scanner. [Online] Available at: <https://nmap.org/>. [Accessed: 2021-04-20].
 - [68] Owasp zed attack proxy. [Online] Available at: <https://owasp.org/www-project-zap/>. [Accessed: 2021-04-20].
 - [69] dex2jar package description. [Online] Available at: <https://tools.kali.org/reverse-engineering/dex2jar>. [Accessed: 2021-04-20].
 - [70] Java decompiler. [Online] Available at: <https://java-decompiler.github.io/>. [Accessed: 2021-04-20].
 - [71] Androguard documentation. [Online] Available at: <https://androguard.readthedocs.io/en/latest/>. [Accessed: 2021-04-20].
 - [72] Apkleaks github. [Online] Available at: <https://github.com/sfahl/mallodroid>. [Accessed: 2021-04-20].
 - [73] Mallodroid github. [Online] Available at: <https://github.com/dwiswant0/apkleaks>. [Accessed: 2021-04-20].
 - [74] Cryptography in mobile apps. [Online] Available at: <https://mobile-security.gitbook.io/mobile-security-testing-guide/general-mobile-app-testing-guide/0x04g-testing-cryptography>. [Accessed: 2021-04-22].
 - [75] S. Siboni, A. Shabati, N. Tippenhauer, J. Lee, and Y. Elovici. Advanced security testbed framework for wearable iot devices. *ACM Transactions on Internet Technology*, vol. 16, pp. 1-25, 2016.
 - [76] R. Das and G. Tuna. Packet tracing and analysis of network cameras with wireshark. *5th International Symposium on Digital Forensic and Security (ISDFS)*, 2017. DOI: 10.1109/ISDFS.2017.7916510.
 - [77] A. Chatxikonstantinou, C. Ntantogian, G. Karopoulos, and C. Xenakis. Evaluation of cryptography usage in android applications. *EAI Endorsed Transactions on Security and Safety*, vol. 3, (9), pp. 1-8, 2016.
 - [78] L. Li, T. Bissyande, M. Papadakis, S. Rasthofer, A. Bartel, D. Octeau, J. Klein, and L. Traon. Static analysis of android apps: A systematic literature review. *Information*

and Software Technology, vol. 88, pp. 67-95, 2017.

- [79] B. Leonardo, C. Berkay, M. Patrick, and U. Selcuk. Real-time analysis of privacy-(un)aware iot applications. *Proceedings on Privacy Enhancing Technologies, vol. 2021, (1), pp. 145-166, 2021.* DOI: <https://doi.org/10.2478/popets-2021-0009>.
- [80] V. Dahl and M. Österlin. Impact of gdpr on data sharing behavior of smart home users: A study on self-disclosure, iot privacy and consumer trust. *Bachelor Thesis in Computer and Information Science, Malmö Univeristy, 2020.*
- [81] S. Spiekermann and L. Faith Cranor. Engineering privacy. *IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, VOL. 35, 2019.*
- [82] Lighttpd. [Online] Available at: <https://www.lighttpd.net/>. [Accessed: 2021-04-26].
- [83] The gsoap toolkit. [Online] Available at: <https://www.genivia.com/products.html>. [Accessed: 2021-04-27].
- [84] Real time streaming protocol(rtsp). [Online] Available at: <https://tools.ietf.org/html/draft-rao-rtsp-00.html>. [Accessed: 2021-04-26].
- [85] Android cryptographic apis. [Online] Available at: <https://mobile-security.gitbook.io/mobile-security-testing-guide/android-testing-guide/0x05e-testing-cryptography>. [Accessed: 2021-04-28].
- [86] Ring's general faq - frequently asked questions. [Online] Available at: <https://support.ring.com/hc/en-us/articles/115004666066-Ring-s-General-FAQ-Frequently-Asked-Questions>. [Accessed: 2021-04-27].

Appendix A

IP geo location

IP GEO LOCATION: Arlo

DNS:

<u>IP</u>	<u>Country</u>	<u>Organisation</u>
23.50.59.177	Sweden	Akamai Technologies
23.50.59.123	Sweden	Akamai Technologies
54.229.254.150	Ireland	Amazon.com Inc
52.208.202.169	Ireland	Amazon.com Inc
52.17.203.126	Ireland	Amazon.com Inc
34.246.205.18	Ireland	Amazon.com Inc
34.241.14.204	Ireland	Amazon.com Inc
34.246.32.176	Ireland	Amazon.com Inc
34.243.231.175	Ireland	Amazon.com Inc

TCP:

23.50.59.123	Sweden	Akamai Technologies
34.243.231.175	Ireland	Amazon.com Inc
52.213.123.196	Ireland	Amazon.com Inc
63.34.147.192	Ireland	Amazon.com Inc
52.208.202.169	Ireland	Amazon.com Inc
54.229.254.150	Ireland	Amazon.com Inc
52.17.203.126	Ireland	Amazon.com Inc
34.246.32.176	Ireland	Amazon.com Inc
23.50.59.177	Sweden	Akamai Technologies
52.218.41.154	Ireland	Amazon.com Inc
52.49.74.119	Ireland	Amazon.com Inc
34.246.205.18	Ireland	Amazon.com Inc
54.220.113.102	Ireland	Amazon.com Inc
54.77.185.130	Ireland	Amazon.com Inc
52.215.10.50	Ireland	Amazon.com Inc
52.209.114.95	Ireland	Amazon.com Inc
52.16.9.27	Ireland	Amazon.com Inc
34.254.79.35	Ireland	Amazon.com Inc
34.251.98.51	Ireland	Amazon.com Inc
52.218.24.106	Ireland	Amazon.com Inc

UDP:

No more connections besides DNS

Figure A.1: Arlo: Geo location for IP addresses communicating with device

IP GEO LOCATION: Foscam**DNS:**

<u>IP</u>	<u>Country</u>	<u>Organisation</u>
52.14.28.120	USA	Amazon.com Inc
3.122.162.58	Germany	A100 ROW GmbH (Amazon)
18.197.251.224	Germany	A100 ROW GmbH (Amazon)
52.14.28.120	USA	Amazon.com Inc
3.19.122.63	USA	Amazon.com Inc
198.16.70.218	Netherlands	FDCServers.net
34.192.135.228	USA	Amazon.com Inc
3.219.6.163	USA	Amazon.com Inc
3.218.19.50	USA	Amazon.com Inc
3.208.43.209	USA	Amazon.com Inc

TCP:

34.236.96.203	USA	Amazon.com Inc
34.255.236.161	Ireland	Amazon.com Inc
3.208.43.209	USA	Amazon.com Inc
34.204.224.132	USA	Amazon.com Inc
34.192.135.228	USA	Amazon.com Inc
3.218.19.50	USA	Amazon.com Inc
52.73.50.236	USA	Amazon.com Inc
52.217.9.188	USA	Amazon.com Inc
3.212.225.112	USA	Amazon.com Inc
3.214.37.162	USA	Amazon.com Inc

UDP:

178.162.199.146	Germany	Leaseweb Deutschland
51.105.208.173	Netherlands	Microsoft

Figure A.2: Foscam: Geo location for IP addresses communicating with device

IP GEO LOCATION: Ring**DNS**

<u>IP</u>	<u>Country</u>	<u>Organisation</u>
35.173.163.137	USA	Amazon.com Inc
34.238.35.186	USA	Amazon.com Inc
34.235.27.180	USA	Amazon.com Inc
3.225.90.171	USA	Amazon.com Inc
34.198.118.230	USA	Amazon.com Inc
52.204.171.209	USA	Amazon.com Inc

TCP

18.233.129.70	USA	Amazon.com Inc
3.212.239.212	USA	Amazon.com Inc
3.217.11.0	USA	Amazon.com Inc
3.222.14.252	USA	Amazon.com Inc
3.248.7.159	Ireland	Amazon.com Inc
3.93.251.178	USA	Amazon.com Inc
34.225.190.22	USA	Amazon.com Inc
34.230.200.207	USA	Amazon.com Inc
34.232.97.128	USA	Amazon.com Inc
34.236.177.237	USA	Amazon.com Inc
34.238.197.228	USA	Amazon.com Inc
34.252.95.49	Ireland	Amazon.com Inc
35.157.238.163	Germany	Amazon.com Inc
35.170.237.138	USA	Amazon.com Inc
35.173.163.137	USA	Amazon.com Inc
50.19.66.83	USA	Amazon.com Inc
52.59.209.78	Germany	Amazon.com Inc
54.172.134.242	USA	Amazon.com Inc
54.175.58.212	USA	Amazon.com Inc
54.209.141.209	USA	Amazon.com Inc
54.210.58.38	USA	Amazon.com Inc
54.235.218.62	USA	Amazon.com Inc
54.237.13.161	USA	Amazon.com Inc
54.237.94.188	USA	Amazon.com Inc
54.85.115.43	USA	Amazon.com Inc
54.85.66.234	USA	Amazon.com Inc
54.87.79.36	USA	Amazon.com Inc
65.9.53.114	USA	Amazon.com Inc
65.9.53.15	USA	Amazon.com Inc
65.9.53.58	USA	Amazon.com Inc

Figure A.3: Ring: Geo location for IP addresses communicating with device

UDP		
34.252.95.49	Ireland	Amazon.com Inc
3.121.234.173	Germany	Amazon.com Inc
3.125.37.42	Germany	Amazon.com Inc
3.248.7.159	Ireland	Amazon.com Inc
35.158.133.220	Germany	Amazon.com Inc
52.59.209.78	Germany	Amazon.com Inc
54.93.228.14	Germany	Amazon.com Inc

Figure A.4: Ring: Geo location for IP addresses communicating with device, part 2

Appendix B

Android application permissions

Arlo
Permissions
android.permission.ACCESS_BACKGROUND_LOCATION
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_DOWNLOAD_MANAGER
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.BLUETOOTH
android.permission.BLUETOOTH_ADMIN
android.permission.CAMERA
android.permission.CHANGE_NETWORK_STATE
android.permission.CHANGE_WIFI_MULTICAST_STATE
android.permission.CHANGE_WIFI_STATE
android.permission.DISABLE_KEYGUARD
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION
android.permission.FOREGROUND_SERVICE
android.permission.GET_ACCOUNTS
android.permission.INTERNET
android.permission.MANAGE_OWN_CALLS
android.permission.MODIFY_AUDIO_SETTINGS
android.permission.READ_CONTACTS
android.permission.READ_EXTERNAL_STORAGE
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.RECORD_AUDIO
android.permission.SYSTEM_ALERT_WINDOW
android.permission.USE_BIOMETRIC
android.permission.USE_FINGERPRINT
android.permission.USE_SIP
android.permission.VIBRATE
android.permission.WAKE_LOCK
android.permission.WRITE_EXTERNAL_STORAGE
com.android.launcher.permission.READ_SETTINGS
com.google.android.c2dm.permission.RECEIVE
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

Figure B.1: Arlo android application permissions

Ring
Permissions
android.permission.ACCESS_BACKGROUND_LOCATION
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.BLUETOOTH
android.permission.BLUETOOTH_ADMIN
android.permission.BLUETOOTH_PRIVILEGED
android.permission.BROADCAST_STICKY
android.permission.CAMERA
android.permission.CHANGE_NETWORK_STATE
android.permission.CHANGE_WIFI_STATE
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION
android.permission.FOREGROUND_SERVICE
android.permission.GET_ACCOUNTS
android.permission.INTERNET
android.permission.MODIFY_AUDIO_SETTINGS
android.permission.READ_CONTACTS
android.permission.READ_EXTERNAL_STORAGE
android.permission.READ_LOGS
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.RECORD_AUDIO
android.permission.VIBRATE
android.permission.WAKE_LOCK
android.permission.WRITE_CONTACTS
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.WRITE_SETTINGS
com.google.android.c2dm.permission.RECEIVE
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE
com.ringapp.feature.geofence.ui.permission.GeofencePermissionsActivity
com.ringapp.permission.C2D_MESSAGE
com.ringapp.permission.CONNECT_TO_DOORBOT_NETWORK
com.ringapp.permission.DOORBOT_APP

Figure B.2: Ring android application permissions

Foscam
Permissions
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.BLUETOOTH
android.permission.BLUETOOTH_ADMIN
android.permission.CALL_PHONE
android.permission.CAMERA
android.permission.CHANGE_WIFI_MULTICAST_STATE
android.permission.CHANGE_WIFI_STATE
android.permission.FOREGROUND_SERVICE
android.permission.GET_TASKS
android.permission.INTERNET
android.permission.MODIFY_AUDIO_SETTINGS
android.permission.READ_EXTERNAL_STORAGE
android.permission.READ_PHONE_STATE
android.permission.RECEIVE_USER_PRESENT
android.permission.RECORD_AUDIO
android.permission.SYSTEM_ALERT_WINDOW
android.permission.USE_BIOMETRIC
android.permission.USE_FINGERPRINT
android.permission.VIBRATE
android.permission.WAKE_LOCK
android.permission.WRITE_EXTERNAL_STORAGE
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE
com.foscam.foscam.permission.C2D_MESSAGE
com.foscam.foscam.permission.JPUSH_MESSAGE
com.foscam.foscam.permission.MIPUSH_RECEIVE
com.google.android.c2dm.permission.RECEIVE
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE
com.meizu.c2dm.permission.RECEIVE

Figure B.3: Foscam android application permissions

