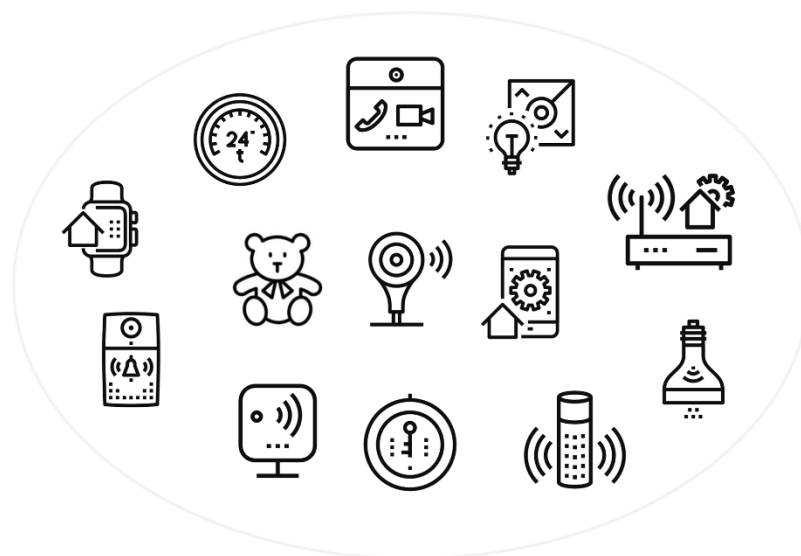


# *The Internet of Things: a privacy label for IoT products in a consumer market*



Cyber Security Academy  
Executive master's program Cyber Security

Author: Rob van Diermen  
Student ID: s1782665  
Date: 08 June 2018  
Supervisor: Jan van den Lubbe – University of Delft  
Second reader: Els de Busser – Leiden University

## Abstract

The IoT market is a very broad market that spans from home automation products to industrial control systems (ICS) and health care systems. The “things” or smart objects in the IoT world provide the interface between the real world and the digital world and the solutions are built upon an entire ecosystem with several stakeholders. The interaction of the IoT products with peoples personal life results in the transmission, processing, and storing of data related to humans, which increases the privacy risk for the users dramatically. The users have no insight in the level of these privacy risks due to the information asymmetry between the suppliers and the users. European and state governmental agencies have proposed several steps to improve this situation. One of the recommendation is to implement a labelling system regarding the security and privacy risks of IoT products. Amongst the other recommendations, the labelling system requires that IoT products need to be tested structurally and consistently for all kinds of IoT products and by different organizations. In addition the security and privacy risks should be assessed consistently.

This thesis is about the design of an IoT privacy label and the methodologies to collect the necessary information to populate the privacy label for an IoT product and its entire ecosystem. The privacy risks of IoT ecosystems are determined by testing all components in the ecosystem for vulnerabilities. These vulnerabilities can be found by security scans, penetration tests and audits, and quantified by using the Common Vulnerability Scoring System (CVSS). The level of the privacy risk can be determined and expressed by combining the sensitivity of the personal information being processed and the vulnerabilities in the IoT ecosystem. A conceptual six layer IoT service model has been developed to better understand the architecture of the IoT product and to structurally test all components.

Three case studies were performed in this research to assess and improve the methodologies and design of the privacy label. Although the design of the privacy label was made with the consumer market in mind, the same label and methodologies can be used for IoT products for businesses and industries.

**Keywords:**

IoT ecosystem, privacy risk matrix, privacy label, IoT Service Model, IoT security testing, Egardia, Woonveilig, Philips Hue Lighting, My friend Cayla.

## Content:

1	Introduction and background.....	5
1.1	The IoT market .....	5
1.2	The government as a stakeholder in IoT security .....	6
1.3	The problem description .....	7
1.4	The research objective and approach .....	8
1.4.1	Case studies and lab environment .....	9
1.4.2	Scope and relevance.....	11
1.4.3	The thesis structure.....	11
2	Measuring information security and privacy risks in the IoT consumer market.....	12
2.1	Assessing the information security and privacy risks in an IoT ecosystem .....	12
2.2	Measuring the vulnerabilities of an IoT system .....	14
2.3	Classification of privacy sensitive data .....	16
2.4	The information security and privacy risk matrix and mitigation strategies. ....	17
2.5	Summary.....	18
3	The design of the Security and Privacy Label .....	19
3.1	The privacy label based on the EU energy label.....	19
3.2	Reeder's Expandable Grid model of the P3P standard. ....	20
3.3	Kelley's proposed Privacy Nutrition Label.....	22
3.4	The IoT privacy label.....	23
3.5	Summary.....	27
4	Testing the components in an IoT ecosystem.....	28
4.1	IoT Architecture.....	30
4.2	The IoT physical device and sensor layer .....	32
4.3	The IoT device network layer .....	33
4.4	IoT controller layer .....	34
4.5	Local network layer .....	34
4.6	Cloud connection layer.....	35
4.7	Cloud application and services layer .....	35
4.8	Summary.....	36
5	Case study 1: Philips Hue lighting.....	37
5.1	Layer 1: The light bulbs and dimmer .....	37
5.2	Layer 2: The ZigBee network .....	38
5.3	Layer 3: The Hue Bridge and app on mobile devices .....	39
5.3.1	Direct Communication between App and Bridge.....	40
5.3.2	Testing the Hue bridge .....	40
5.3.3	Testing the Hue app for Android .....	41

5.4	Layer 4 and 5: the local network and cloud connection layers .....	43
5.5	Layer 6: Cloud application and services layer .....	44
5.6	Summary of issues.....	46
5.7	The privacy label for the Philips Hue light system .....	48
6	Case Study 2: The Egardia alarm system .....	49
6.1	Layer 1: The alarm sensors and controllers.....	49
6.2	Layer 2: The wireless sensor network .....	51
6.3	Layer 3: The alarm gateway .....	52
6.3.1	Communication between gateway and cloud services.....	52
6.3.2	Penetration testing on the Egardia gateway.....	52
6.3.3	The Egardia App.....	52
6.4	Layer 4 and 5: The local area network and cloud access layer .....	54
6.5	Layer 6: Cloud application and services .....	54
6.6	Summary of issues in the Egardia ecosystem .....	57
6.7	The privacy label for the Egardia Alarm system.....	59
7	Case study 3: The doll “My friend Cayla” .....	60
7.1	Layer 1 and 2: The doll Cayla and the Bluetooth connection.....	61
7.2	Layer 2: The sensor network .....	61
7.3	Layer 3: The Cayla app on a mobile device .....	61
7.4	Layer 4 and 5: The local area network and cloud connection layer.....	64
7.5	Layer 6: Cloud services for Cayla .....	64
7.6	Summary of identified issues .....	65
7.7	The IoT privacy label for Genesis’ My Friend Cayla.....	67
8	Conclusion, recommendations and reflection .....	68
8.1	Recommendations.....	68
8.2	Further research.....	69
	Bibliography.....	70
	Appendix A: MitM attacks on Philips Hue and Egardia alarm systems.....	75
	Appendix B: Philips Hue Bridge Internal Debugger.....	77
	Appendix C: Device information send to data.flurry.com by Philps Hue .....	79

## 1 Introduction and background

The Internet of Things (IoT) is a broad concept of intelligent devices and services that exchange data over new and existing networks often provides an interface between the physical and digital world. The following definition for IoT was given in 2012 by the ITU Global Standards Initiative: *“The Internet of Things (IoT) has been defined in Recommendation ITU-T Y.2060 (06/2012) as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.”*[1]. The IoT could also be described as: *“The network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to connect and exchange data”*[2].

Compared to PCs, laptops, tablets and mobile phones, that have many different applications, IoT devices generally have only a limited set of functions. They come, however, often with a set of applications and services (the IoT ecosystem) providing remote communication, data processing, and user interaction. For example a wearable device is used to register heart rates, location and motion. The collected data is sent to a service provider that processes the data into meaningful information for the user of the wearable. An intelligent thermostat, such as the NEST thermostat, provides the ability to remotely control the thermostat from anywhere using the Internet, an app or browser, and a local Wi-Fi connection[3]. Furthermore, the thermostat uses activity sensors and the location of cell phones to determine if somebody is home or not[4]. In both cases sensitive information such as health related and location information is recorded, transmitted to and stored in various places.

In line with the definitions given above, IoT devices are computing devices that have network interfaces, complete protocol stack(s) and application(s) running on top of it. The main difference with PCs, laptops, tablets and smart phones, however, is that these IoT devices have no end-point protection facilities such as virus scanners and host based firewalls. Especially in the consumer market, the IoT devices need to be low priced and user friendly, i.e. plug-and-play and connect automatically. As a result, manufacturers of IoT devices have to balance between the costs, usability and security of the device. Balancing between these three aspects means an inherent risk of limited security in favour of usability and/or costs. In addition, manufacturers have to comply with technical standards to be interoperable to with other IoT devices. For example Philips lighting system Hue works with a variety of systems such as smart assistants from Amazon, Google, Apple and Microsoft as well as alarm systems and home automation products from Nest [5][6].

### 1.1 The IoT market

A strong growth of connected devices is expected for the coming years. Garner estimated a 6,4 billion devices connected in 2016, a 30% growth over 2015[7]. While the initial expert estimations of 50 billion connected devices in 2020 were overestimated, they still expect a number between 20 and 30 billion of connected IoT devices[8]. Generally the IoT market can be divided in a market for consumers and a market for business as shown in the figure below[9]. In this model there is a clear separation between the consumer-facing (IoT2C) and business-facing (IoT2B). While the abbreviation IoT is universal in the literature, there is a plethora of abbreviations for the branches are also called Consumer IoT (CIOT) and Industrial IoT (IIOT).

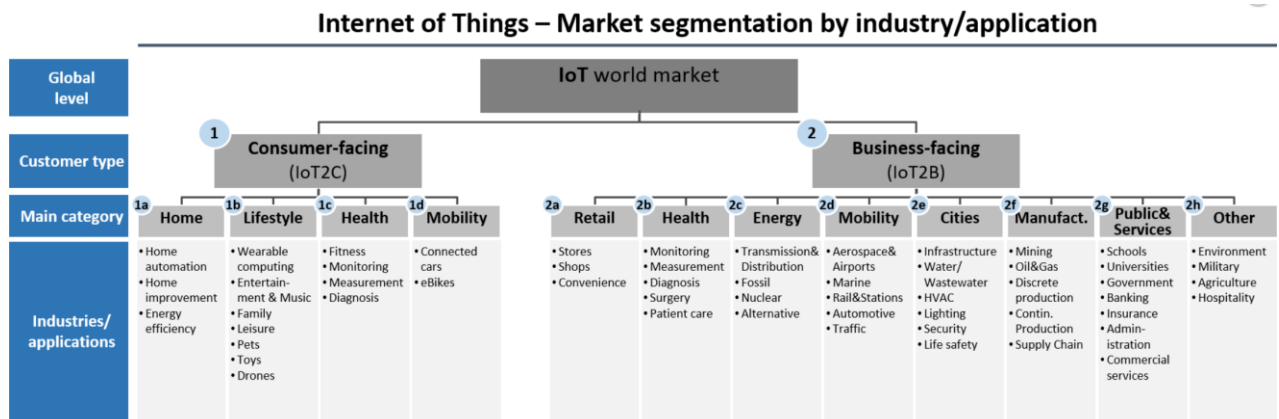


Figure 1: IoT Market segmentation[9]

While similar technology is often used in both branches, there is a difference in devices. IoT in the consumer market are typical devices and appliances in the area of consumer electronics such as smart watches, smart TVs, toys, and smart home products[10]. On the other side, the new IoT technologies have led to many new appliances in the business area. Especially the development of special sensors and the use of RFID technology has led to many innovate solutions in health and manufacturing. The business-facing IoT market is much larger in terms of money and in terms of adoption due to the availability of a wide range of applications in organizations[11].

As shown in figure 1, the main areas of IoT in the consumer market are:

- Home – Home automation is referring to things in a home that can be programmed to function in a particular way. Popular applications in home automation are light bulbs, switches, home security and climate control.
- Life style – This category contains various types of devices, including smart watches and toys. The new “Voice Assistants” type of devices such as Google’s Assistant, Amazon’s Alexa, Apple’s Siri, and Microsoft Cortana fall also in this category. While these assistant services were available for several years on PCs and mobile devices, they now come in dedicated hardware appliances[12].
- Health – Fitness equipment and simple hart rate monitors are used for sports enthusiasts and have a close link with the wearables. More professional body sensors are used by caregivers to monitor their patients from any location[13].
- Mobility – Cars, motorcycles and e-bikes are equipped with motion sensors, GPS and mobile network connections to improve safety of the driver and vehicle.

Privacy risks are a significantly higher in the consumer markets than business markets due to sensitivity of data that is processed and the implemented security controls. The sensors of IoT devices in the consumer market are often collecting personal data and privacy-sensitive information as they are designed to support and improve the user’s private life. In the business market there is generally more process information collected by IoT and less personal data. Furthermore, organizations in the business market are likely to have more knowledge and processes available to manage the security of IoT devices. It cannot be expected from an average consumer to have sufficient technical knowledge to assess the security and privacy risks of an IoT ecosystem. Compared to traditional IT, consumers nowadays know that computers, tablets and smart phones frequently receive software updates and that these updates are necessary to maintain the security of the device. Users of personal computers know that anti-virus and malware detection is necessary for protection of the data stored on the device.

## 1.2 The government as a stakeholder in IoT security

Important stakeholders regarding the security and protection of privacy in IoT ecosystems are of cause the consumers and organizations in the supply chain of the IoT products and services. Consumers could be informed about the security and privacy risks of the products through a labelling system, similar to the

EU energy label that classifies electric equipment based on their energy consumption. Manufacturers and service providers in the supply chain can differentiate themselves from the competition with better security and privacy policies.

Governments on EU level as well as individual state level can enforce the broad implementation of such a privacy label through legislation that forces the supply chain towards the delivery of more secure products and more transparency regarding their privacy practices. The Dutch Cyber Security Council made the following six strategic recommendations to the Dutch Ministry of Justice and Security to coop with the IoT's security threats to the society [14]:

1. *Certification to keep insecure devices from the European market.*
2. *Increase transparency by funding an independent monitor of hacked and vulnerable devices that will publish information on manufacturers and suppliers who do not protect their devices adequately.*
3. *Awareness raising through a labelling system that informs users about the level of security, if the device can receive updates, the period during which the supplier will maintain the product, and if the device can be disconnected from the Internet without loss of 'normal' functionality.*
4. *Increased product liability for the security of the products and services, whereby manufacturers can be held liable for the economic losses.*
5. *Clear responsibilities of intermediaries by adding industry guidelines for IoT security under the existing duties of care for intermediary suppliers.*
6. *Improving enforcement by proper mandates and capacity for supervisory authorities to guarantee the enforcement of cybersecurity standards and rules in all sectors.*

The Radiocommunications Agency within the Dutch Ministry of Economic Affairs and Climate policy argues for minimum security requirements and standards of IoT systems[15]. The European Commission and the European Union Agency for Network and Information Security (ENISA) have also created proposals for certification of devices and services in the European Cybersecurity act and the security baseline requirements for IoT [16][17]. The Dutch and EU proposals have a main focus on cybersecurity, which plays a crucial role in the protection of a persons' data and privacy. A person's privacy could be violated and personal data could be leaked in case of a security breach in an environment where this data is processed. Therefore, the security of an IoT ecosystem is a prerequisite for privacy.

The security of an IT or IoT product is not static, without proper maintenance the security of a product will deteriorate over time. A product can be compliant with the highest security standards today, but become vulnerable over time when not maintained well. The security level of an IoT product should therefore be monitored and reported upon through either the proposed monitoring organization or through self-assessment of the manufacturers and suppliers. This information should be publicly available online.

All the recommendations and proposals regarding IoT security and privacy given by the Dutch ministries, the European Commission and ENISA require that the security of the IoT ecosystems are measured or assessed and the citizens should be informed about this. A labelling system is one of the means to provide the consumer with relevant security and privacy related information.

### 1.3 The problem description

Managing the security and privacy of IoT products will become an issue in the near future given the strong growth and increasing capacity of the devices (more sensors and more data collection), and the inherent weak security measures. Customers of IoT products are generally not aware of the security and privacy risks they are facing when buying and using an IoT device because they have no insight in strengths and weaknesses of the security measures and privacy protection mechanisms in an IoT ecosystem. This lack of insight applies to the consumer market as well as to the industrial market for health care devices such as peace makers and medicine pumps. The Dutch and EU agencies recommend a certification and labelling

system that would inform consumers adequately but the agencies did not include any recommendations or requirements regarding these aspects of the security governance.

Insight in the security of IoT devices can be obtained by performing security tests and assessments, which in turn raises the questions: “What and how to test and to report?” Answers to these questions depend on an number of variables, including: the level of assurance that needs to be given by the researcher, the needs of the intended users and the responsible parties, the data involved (confidentiality, integrity, availability, non-repudiation), the technologies used in the ecosystem, and the accessibility of the devices and services to the researcher.

There are industry best practices such as the OWASP Internet of Things Project that provides an IoT Framework Security Considerations and IoT Testing guides[18][19]. ENISA’s Baseline Security Recommendations for IoT also provides 73 high-level security measures and good practices [17, pp. 46–52]. These guidelines are, however, an enumeration of security practices and aspects to be tested without any context.

#### 1.4 The research objective and approach

The main objective for this research is to design a labelling system that gives consumers insight in the security and privacy risks related to an IoT eco-system and the methodology to obtain the required data for the labelling system.

The overall research approach is based on Design Science for the development of the privacy label and the necessary methodology to assess the security and privacy risks. “*Design science supports a pragmatic research paradigm that calls for the creation of innovative artefacts to solve real-world problems. Design science research must produce a viable artefact in the form of a construct, a model, a method, or an instantiation*”[20].

Four phases were used in this research by deriving research questions from the main objective:

1. *How can the security and privacy risks of an IoT ecosystem be qualified or quantified in a consistent manner?*

The security and privacy risks have to be qualified and/or quantified to be able to present the outcome in a label. With the input of literature research, a privacy diagram has been developed that shows the relationship between vulnerabilities in the system and the privacy risk. The vulnerabilities of an IoT system can be measured and qualified by the Common Vulnerability Scoring System (CVSS) [21]. By classifying an IoT ecosystem based on the level of personal information is processed, the privacy risk can be qualified in terms of:  
 $\text{privacy risk} = (\text{vulnerability level}) \times (\text{amount of personal information}).$

2. *What information should be presented in a privacy label for the customers and how should this information be presented?*

Literature study is used to explore the existing labelling models and their strengths and weaknesses. A new privacy label is designed by using existing labelling models, building upon their strengths, and tailoring it to the IoT world.

3. *How to test the security levels in an IoT ecosystem?*

A single IoT ecosystem is built upon a large numbers of systems, technologies, and services from different providers. Insight in the architecture of the IoT’s ecosystem is therefore very important. A conceptual six layer IoT service model is developed to identify the security weaknesses and privacy risk at each level. For each layer the specific risks are identified which provides guidance in the security tests and scans that should be performed at that layer.



4. *Can we use the designed models from previous questions in a variety of IoT products?*

The main objective is to have a single privacy label that can be applied to all kinds of IoT system or even to a broader set of IT applications and services. Three case studies took place in this research to verify the methodology to test for vulnerabilities in the IoT ecosystem, translate these identified vulnerabilities into a security risks to populate the privacy label.

A graphical overview of the research approach is given in the figure below.

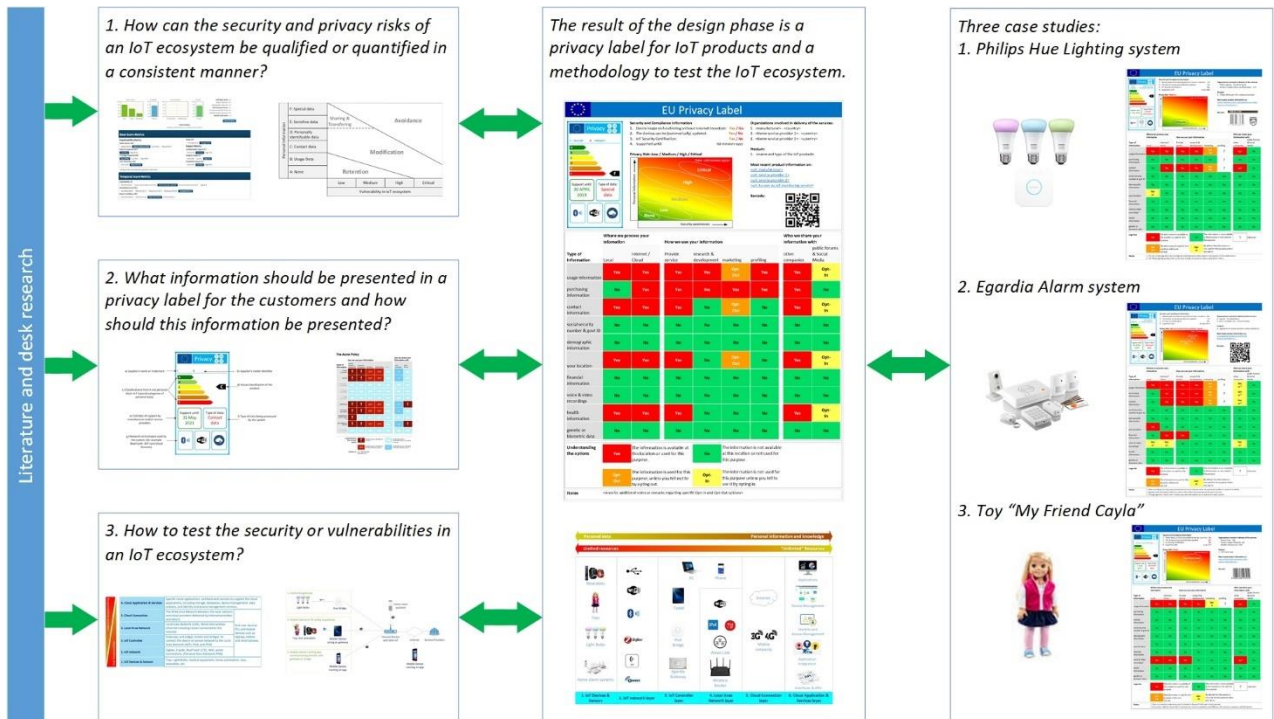


Figure 2: Research Overview

The final design presented in this thesis was developed in an iterative process, shown by the bidirectional arrows in the figure above. Literature and desk research provided the input and starting point for answering the first three research sub-questions. The first three phases produced a methodology to qualify privacy risk, a design for the privacy label, and a methodology to structurally test the IoT ecosystems. The methodologies were used in three case studies to populate the privacy label for different IoT ecosystems. The methodologies and label were updated based on the experience acquired in the case studies.

1.4.1 Case studies and lab environment

A significant part of this research is based on experiments on the security of actual IoT products in the consumer market. The following criteria were applied in the selection of products to test the applicability of a privacy label:

- The product should be sold on the Dutch market through retail shops in order to make the investigations and outcomes more relevant for consumers.
- There should be some product or brand awareness of the product.
- The product should leverage an ecosystem including cloud services and mobile apps in order to investigate the impact of the ecosystem on the privacy risks.
- The products should fall into different categories, e.g. wearables, smart lightning, alarm system, health, etc.

Literature and desk research was used to select the following three products that were used in this experiment:

1. Philips Hue lighting system[5]. Philips Hue was introduced in 2012 and was the market leader in connected home lighting in 2016[22].
2. Home alarm system by Egardia[6]. The alarm system is branded as Woonveilig Alarm in the Netherlands and is recommended by Dutch television programs Vara “Kassa”, RTL4 “MediaZine”, SBS 6 “Tuinruimers”, and the magazines “Beste Koop”, “Computer Totaal”, “Computer Idee”, and “Quest”[23].
3. Genesis toy “My friend Cayla”[24]. The toy was sold in many different countries but was banned from the German and Dutch market due to its security flaws[25].

The Philips Hue lighting and Egardia alarm system starter kits were sold as a package deal on the Dutch market for €299,-- and the Genesis Toy was bought for €25 earlier in 2016 for a separate research project.

A lab environment was created to test the three IoT devices. An overview of the lab is given in the figure below.

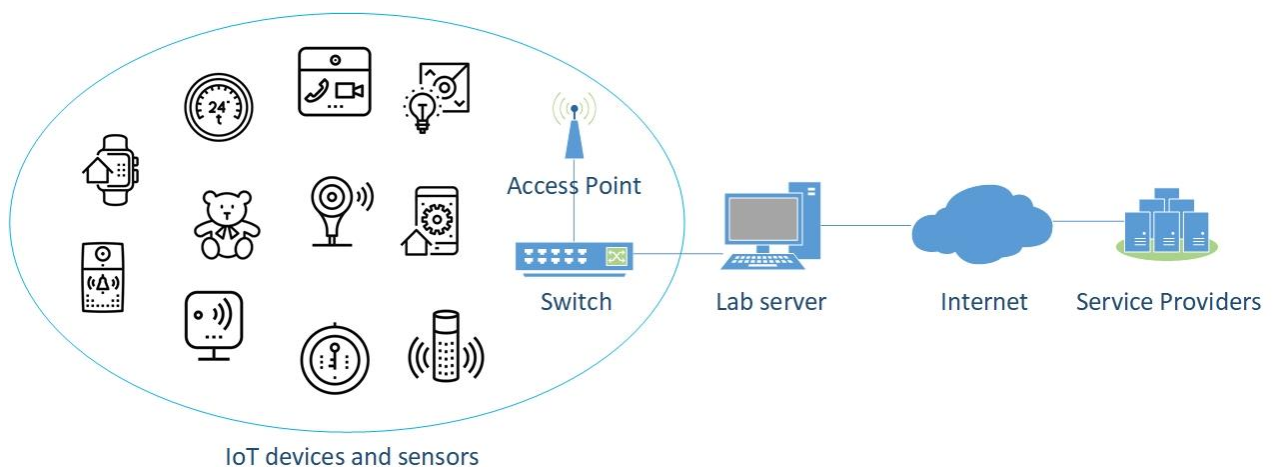


Figure 3: Overview of the lab environment

The lab consists of the following components:

1. The lab server running Kali Linux (2017.3) with two interfaces, one connected to the Internet and one connected to the lab network switch.
2. The lab network switch is a NetGear GS105 with port mirroring to the port connected to the lab server so that network traffic from the wireless access point and multiple IoT devices connected to the switch can be analysed with Wireshark on the lab server.
3. Ubiquiti Unify Access point to connect mobile devices using WiFi to connect directly to the IoT devices and to communicate to the Cloud Applications.
4. A lab workstation running Virtual Machines, including:
  - a. Pentoo and a Software Defined Radio, GNU radio and supporting libraries for HackRF One [26] [27].
  - b. Mobile app code review tools, including Mobile Security Framework to perform code analysis of the apps, Quixxi, and Osterlab online services[28][29][30].
  - c. Kali Linux with ZigBee dongle and Killerbee software to inspect ZigBee traffic (RZ USBstick)
5. Asus tablet running Android 7.0 to run the mobile apps.

The level of security and privacy protection measures were tested at each level of the IoT service model.

#### 1.4.2 Scope and relevance

The scope of this research is limited to IoT systems in a consumer market. The same approach can be used for the security assessment of products in the industrial market. The designed methodology to assess the security of IoT ecosystems should help IT security specialists and practitioners, such as pen testers, researchers, and auditors to adequately test the security of IoT ecosystems and clearly report the outcome.

The web applications and cloud services are an important part of the IoT ecosystem that pose a direct privacy risk to the user. A security assessment of the service providers' systems and processes is necessary for the content of the privacy label. These aspects were, however, not tested for the products used in the case studies. Active security scanning, penetration testing, and reviewing the supplier's internal processes do require the collaboration and approval of the supplier. The identified security weaknesses in the case studies are therefore limited to what can be inspected passively on the user's side of the IoT ecosystem.

#### 1.4.3 The thesis structure

This first chapter introduced the subject of thesis. The first part described the context and the problems that the IoT ecosystems are facing and the initial actions from governmental agencies to improve the security and privacy of the citizens. The second part described the objectives for this research and how this was achieved. Each of the research sub-questions and case studies are described in the following chapters.

- Chapter 2: Measuring information security and privacy risks in the IoT consumer market
- Chapter 3: The design of the Security and Privacy Label
- Chapter 4: Testing the components in an IoT ecosystem
- Chapter 5: Case study 1: Philips Hue lighting
- Chapter 6: Case study 2: The Egardia Alarm System
- Chapter 7: Case study 3: The toy "My Friend Cayla"
- Chapter 8: Conclusion, Recommendations and Reflections
- Bibliography
- Appendix A: MitM attacks on Philips Hue and Egardia alarm systems
- Appendix B: Philips Hue Bridge Internal Debugger
- Appendix C: Device information send to data.flurry.com by Philips Hue.

## 2 Measuring information security and privacy risks in the IoT consumer market

The IoT market is a very broad market that spans from home automation products to industrial control systems (ICS) and health care systems. The “things” or smart objects in the IoT world provide the interface between the real world and the digital world which leads to a unimaginable number solutions and implementations. These solutions are built upon an entire ecosystem with several stakeholders. The interaction of the IoT products with peoples personal life results in the transmission, processing and storing of data related to humans. *“It depicts the edge between person and technological ecosystem nodes and originates from the necessity of protecting data related to humans. In IoT, it is essential to fulfil privacy requirements due to the omnipresence of intelligent objects, and the risk of technology mishandling by legitimate and/or illegitimate users”*[31].

It is clear that privacy of humans needs to be protected and there is an inherent risk that the privacy sensitive data is disclosed to unauthorized persons when this data is stored, transported, and processed in IT systems. There can be various reasons for the undesired disclosure, including weak security processes at service providers and adversaries who exploit one or more vulnerabilities in the ecosystem. In order to assess the privacy risks related to IoT products in the consumer market it is necessary to get an understanding what privacy risk is and how it can be assessed.

### 2.1 Assessing the information security and privacy risks in an IoT ecosystem

The ISO/IEC 29100 – Privacy framework defines privacy risk as: “The effect of uncertainty on privacy” where uncertainty is *“the state of deficiency of information related to an event, its consequence, or likelihood”* [32, p. 3]. A definition of privacy is not given in this standard. However, many definitions of privacy can be found in dictionaries and literature and include *“Someone’s right to keep their personal matters and relationships secret”*<sup>1</sup>, *“A state in which one is not observed or disturbed by other people”*<sup>2</sup>, *“Privacy is the ability of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively”*, and *“The right to be let alone”*<sup>3</sup>. A more specific definition in the realm of information systems is captured in *“Information Privacy: Also known as data privacy, is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them”*[33, p. 259].

Based on the definitions above the information or data privacy is about the protection of personal data. Personal data is defined in the new European Union’s General Data Protection Regulation (GDPR) as *“any information that relates to an identified or identifiable living individual”*[34]. Examples of personal data or the often used term personally identifiable information (PII) are: name and surname, home address, email address, identification card or passport number, location data, phone numbers, gender, nationality etc. The following definition of privacy risk in the context of IoT could be derived from the various definitions and descriptions of privacy and risk: **“The risk of undesired disclosure of information about humans”**. Information about humans includes their PII as well as their behaviour that can be monitored and tracked.

The level or magnitude of a security breach is *“expressed in terms of the combination of consequences and their likelihood, where the likelihood is the chance of something happening”*, similar to an information security risk [35]. The chance that a security or privacy breach occurs is equally important as the impact that a potential breach might have in a risk assessment. This likelihood is determined by the threats, for example individual hackers that want to steal and sell personal information, the vulnerabilities in the IoT’s

<sup>1</sup> <https://dictionary.cambridge.org/dictionary/english/privacy>

<sup>2</sup> <https://en.oxforddictionaries.com/definition/privacy>

<sup>3</sup> <https://en.wikipedia.org/wiki/Privacy>

ecosystem and the effectiveness of preventive controls. The coherency of threats, preventive controls, a privacy breach, repressive controls and consequences is given in the conceptual Bow Tie diagram below[36].

The different causes of unwanted events are given as a threat on the left side of the bow tie diagram. These threats and vulnerabilities are eliminated by preventive controls, i.e. the absence or ineffective preventive controls increases the likelihood that a threat materializes into a security and a personal data breach. On the left side of the model a few of the possible

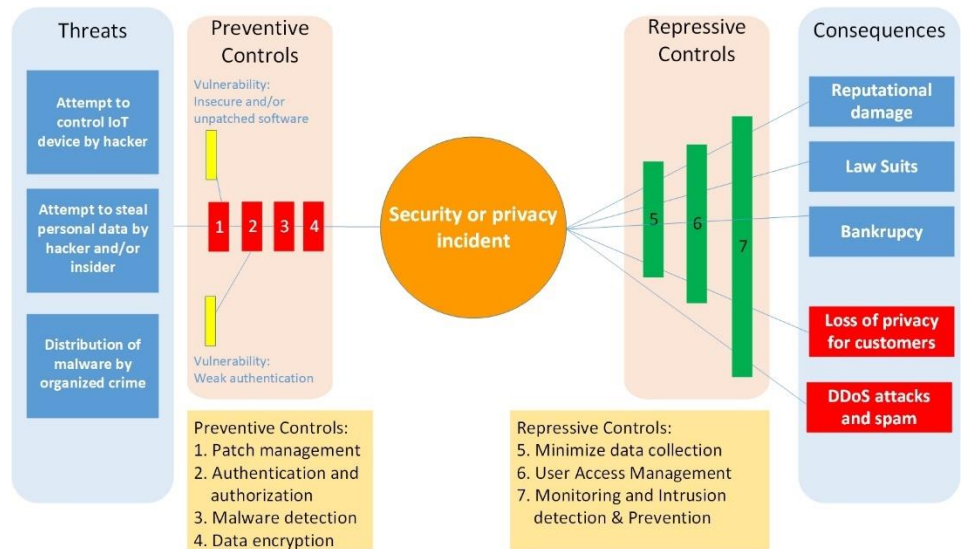


Figure 4: Conceptual Bow Tie diagram for IoT security and personal data breaches [19]

consequences are given for the manufacturer, the customers and the victims of a DDoS attack and spam. Repressive controls mitigate the consequences or impact once a breach has occurred, these controls do not limit the likelihood of an event. As shown in the Bow Tie diagram, the likelihood of an incident increases when the IoT system has vulnerabilities or ineffective controls that can be exploited by adversaries. For example, the lack of data encryption allows an adversary for to perform a man-in-the-middle attack and eavesdrop on confidential data, including user credentials, that in turn can be used on other systems to get more data.

Privacy risk in an IoT environment could be seen as a risk category within information security risks, based on the model above. A security breach could lead to a privacy breach but a privacy breach in an IoT ecosystem is unlikely without an information security breach caused by vulnerabilities in people’s behaviour, system management processes and technology. The factor “likelihood” used in the definitions of information security and privacy risks is very hard to calculate due to the large number of variables in an IoT ecosystem. In qualitative assessments, the likelihood will subjective to the experience and beliefs of the individuals performing the assessment[36]. In a security and privacy labelling or classification system it is necessary that the assessment of information security and privacy risks are performed consistently and repeatable for all kinds IoT ecosystems and by different organizations.

Vulnerabilities in an IoT ecosystem could provide a measurable and transparent replacement for the likelihood factor in the risk assessment because these vulnerabilities highly influences the likelihood of a security and privacy breach. The vulnerabilities of software, hardware and firmware can be measured through penetration testing. The vulnerabilities in manufacturers and service providers’ people and processes can be assessed through internal and external audits. By using vulnerabilities as discriminating factor, the level or magnitude of a privacy risk of an IoT system can be expressed in terms of the combination of the amount and sensitivity of personal information and the vulnerabilities in an IoT system. As shown in the privacy risk matrix in figure 5, the privacy risk increases from none towards critical with increased vulnerabilities and an increased amount and sensitivity of personal information that is at risk through vulnerability.

The GDPR describes a personal data breach as: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed” [34, p. 34]. This includes the information security attributes, confidentiality integrity and availability. The requirements for confidentiality integrity and availability (CIA) of the personal data is different for each IoT product. For example, The CIA requirements for an healthcare IoT solution are likely to be higher than the requirements for a smart lighting system.

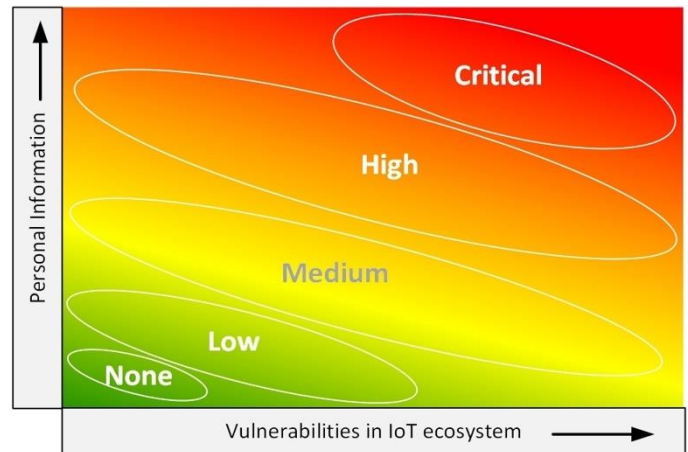


Figure 5: Privacy risk matrix

## 2.2 Measuring the vulnerabilities of an IoT system

An industry standard to define vulnerabilities of software, hardware and firmware is the Common Vulnerability Scoring System (CVSS)[21]. CVSS is developed and maintained by the Forum of Incident Response and Security Teams (FIRST) founded in 1990 as a response to emerging Internet worms. The current version CVSS v3 provides a quantitative model to measure vulnerabilities in a consistent and repeatable way. The scoring system captures the characteristics of a vulnerability and provides a numerical score on a scale from zero to ten and a textual representation of the used CVSS metrics. Subsequently this scoring method can be translated in to the qualitative representation as shown in the table below[21]. The CVSS severity scores can be used by organizations to provide an easier to understand classification and prioritize the remediation of the vulnerabilities.

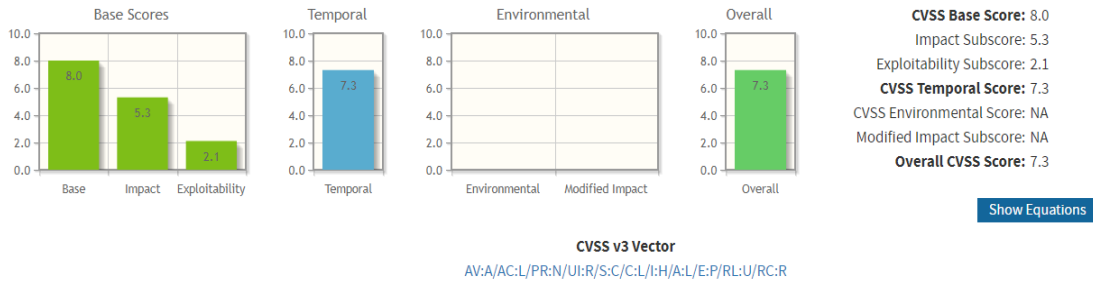
Table 1: Qualitative severity rating scale[21, Sec. 5].

CVSS Score	Severity rating
0.0	None
0.1 – 3.9	Low
4.0 – 6.9	Medium
7.0 – 8.9	High
9.0 – 10	Critical

The CVSS score is based on 15 metrics in three main metric groups: base, temporal, and environmental. The base metric group has eight metrics that cover:

1. The exploitability metrics that measure the complexity and technical means of the vulnerability.
2. The impact metrics that measure the direct impact on confidentiality, integrity, and availability of a successful exploit.

The temporal metric group has three metrics that measure the state of exploit techniques (is the exploit code publicly available?), are patches or mitigating workarounds available, and the confidence in the existence of the vulnerability. The environmental metric group has four metrics that allow for customization or tailoring of the CVSS scores by measuring the additional and alternative controls in place. The temporal and environmental metrics are optional in a CVSS score. A CVSS score gives a qualitative representation of a vulnerability in software, hardware, and firmware. Especially the Base Score metrics in a CVSS score implicitly represent the “likelihood” of a security breach. The likelihood of a security breach increases when functional exploit is available on the Internet that remotely exploits one or more vulnerabilities in an IoT ecosystem. An example of an CVSS calculation is shown in the figure 6.



### Base Score Metrics

**Exploitability Metrics**

Attack Vector (AV)\*  
 Network (AV:N)  Adjacent Network (AV:A)  Local (AV:L)  Physical (AV:P)

Attack Complexity (AC)\*  
 Low (AC:L)  High (AC:H)

Privileges Required (PR)\*  
 None (PR:N)  Low (PR:L)  High (PR:H)

User Interaction (UI)\*  
 None (UI:N)  Required (UI:R)

**Scope (S)\***  
 Unchanged (S:U)  Changed (S:C)

**Impact Metrics**

Confidentiality Impact (C)\*  
 None (C:N)  Low (C:L)  High (C:H)

Integrity Impact (I)\*  
 None (I:N)  Low (I:L)  High (I:H)

Availability Impact (A)\*  
 None (A:N)  Low (A:L)  High (A:H)

\* - All base metrics are required to generate a base score.

### Temporal Score Metrics

**Exploitability (E)**  
 Not Defined (E:X)  Unproven that exploit exists (E:U)  Proof of concept code (E:P)  Functional exploit exists (E:F)  High (E:H)

**Remediation Level (RL)**  
 Not Defined (RL:X)  Official fix (RL:O)  Temporary fix (RL:T)  Workaround (RL:W)  Unavailable (RL:U)

**Report Confidence (RC)**  
 Not Defined (RC:X)  Unknown (RC:U)  Reasonable (RC:R)  Confirmed (RC:C)

Figure 6: Example of a CVSS score calculation<sup>5</sup>.

In this example the online calculator provided by NIST was used<sup>4</sup>. The tree main metric groups and the overall score is provided in the top section. In this example the CVSS score is calculated for an alarm system sensor network vulnerable for a replay attack of the key-fob’s disarming and arming RF signals, allowing an adversary to capture these RF signals and replay them with the appropriate tooling. The vulnerability is exploitable through the adjacent network, i.e. the local RF sensor network. Given the appropriate tooling, the attack complexity is relatively low. It does however require a user to use the key-fob ones to enable and disable the alarm for the recording. Once recorded, the adversary can replay the signals as often as he wants. In this example the base score of 8 is reduced by the temporal score in the overall score to 7.3 (high) because the Exploitability is set to “Proof of Concept” and the Confidence level is set to “Reasonable”. The CVSS v3 Vector “AV:A/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:L/E:P/RL:U/RC:R” provides the vulnerabilities characteristics<sup>5</sup>.

The environmental measures were not used in this example as there were no additional mitigating controls. A complete overview of each metric, value, and score calculation per metric group is provided in the CVSS v3 specification document [21, Sec. 8].

Service providers in an IoT ecosystem are an attractive target for adversaries who want to steal personal data on a large scale. Where the individual IoT system reveals personal information of a very limited number of users in a household, the service providers collect, process and store the personal information for all their customers. The maturity of the service provider’s service and security management processes also play a vital role the IoT ecosystem. Weak secure software development, release and change

<sup>4</sup> <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

<sup>5</sup> <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:L/E:P/RL:U/RC:R>

management processes could lead to critical security incidents[37][38]. In theory the vulnerabilities in the service provider's processes could be plotted in the privacy risk matrix, similar to the technical vulnerabilities. The problem is that insight in the provider's weaknesses is hard to get because:

- There is no obligation for a service provider to publish its known issues and weaknesses regarding internal processes if they are known at all. But even if the service provider has performed penetration tests as part of the secure software development processes, there is no assurance that the issue is resolved when the product is brought to the market.
- Independent security researchers cannot launch a penetration test on the service provider's systems because this is legally not allowed without permission of the owner. This aspect becomes even more complex when multiple service providers are involved to deliver different services. For example, the manufacturer is accountable for the overall security of the IoT solution. However the manufacturer can outsource large parts of the entire operation. The backend services might running on a Platform as a Service (PaaS) from one provider and hosted on Microsoft's Azure or Amazon's AWS infrastructure. The software on top of the operating system and database delivered by the PaaS could be developed and managed by a 4th service provider. Obtaining approval for a penetration test in such an environment can be a daunting task.

These problems and solutions are further discussed in paragraph 4.7.

### 2.3 Classification of privacy sensitive data

As shown in the privacy risk matrix in figure 2, the amount and sensitivity of personal information determines the impact of an incident. The disclosure of video footage from surveillance cameras or any kind of personal conversation is more severe than the disclosure of the usage data of a specific device that can hardly be related to a person. Classification of privacy sensitive or personal data is therefore necessary to determine the impact of a potential security breach. Based on various privacy policies and the GDPR the following six classes of personal data are defined [39][40][34].

Table 2: Classification of personal information processed by IoT ecosystems.

Class	Type of shared data	Description
<b>A</b>	None	The IoT device has intelligence but is not connected, or is only connected to retrieve data anonymously, i.e. no risk from a privacy perspective. For example the anonymous retrieval of software updates of the device.
<b>B</b>	Usage data	Some form of usage data is collected from the device and processed anonymized by the service provider.
<b>C</b>	Contact Information	This category includes the contact information such as email address, address, phone number(s). For example, a service that requires an account with a valid email address or phone number is necessary for the functionality of the device should be classified as "C". This category of data can be anonymized in one or another way.
<b>D</b>	Personal identification data	This type of data can be used directly in the identification of a person and includes for example the name, surname, date of birth, social security number.
<b>E</b>	Sensitive data	This type of data includes financial data such as credit card and bank account information, video and voice recordings, location of a user, and toys play data. Play data are the recordings made by the toy, voice as well as video or photographs, while the child was playing with the toy. Due to its sensitivity, this requires stronger security measures compared to the lower categories of personal account data.
<b>F</b>	Special categories of personal data	This category is specified in Article 9 of the General Data Protection Regulation and includes racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation[34, p. 38].



Because category A and B have no personal or anonymized data the privacy risk would be low when the usage data cannot be related to a person or location (home address). Even when the IoT ecosystem has critical vulnerabilities the privacy risk is low when there is no or very limited personal information processed, stored, or transmitted. The privacy risk increases for class B systems for example when the location of the IoT device is known, for example through wardriving. In these cases the type of personal data that is disclosed in the proximity of a house determines the privacy risk.

## 2.4 The information security and privacy risk matrix and mitigation strategies.

Adversaries could exploit critical vulnerabilities in the IoT ecosystem, for example to launch further attacks on adjacent systems within the house or deploy malware. This malware can be part of a botnet to launch massive DDoS attacks on the Internet or used to distribute spam[41]. The threat of the DDoS and spam malware create a negative externality for other Internet users, because the consumers and manufacturer of a vulnerable IoT system will probably not face the consequences of the malware on their systems[42]. Improving the security measures in the IoT ecosystem will therefore not only mitigate the privacy risks, but will also reduce the likelihood of successful attacks on other systems of the owner as well as other systems on the Internet.

Especially the manufacturers and service providers in a IoT ecosystem should have risk management processes in place, including a risk treatment strategy. Risk treatment is all about how the identified risks will be handled. An organization as well as the end user can evaluate additional security measures and controls to reduce the risk by reducing the impact, reducing the likelihood, or both. The purpose of the anticipated information security and privacy risk label is to inform the users about the risk so they can decide if they want the product and to what extent they want to use it. In general there are four types of risk treatment[35, Sec. 9] that can be applied by all stakeholders in their own context:

1. Risk avoidance – the identified risk is not acceptable and the product cannot be released in its current stage and the cost for repairing are too high. In such a case, the manufacturer and service providers can decide to withdraw the product or specific services entirely. An owner might not buy the product or decommission it completely if the risk is (gone) beyond his appetite.
2. Risk modification – the risks are beyond the risk appetite but can be reduced to an acceptable level by implementing additional controls and measures. For example, manufacturers might implement stronger encryption of personal data and stronger authentication and authorization mechanisms to mitigate the risks of eavesdropping on confidential information. A service provider might implement intrusion detection and prevention systems (IDS/IPS) to detect and prevent attacks in an early stage. A user might for example decide to use the product locally without using the Internet service. A more IT savvy user could create a separate network segment at his home for IoT devices and apply a firewall with specific rules to restrict communication to and from the IoT devices.
3. Risk retention – the risk is within the risk appetite and therefore accepted without any additional measures. Manufacturers and service providers should however still investigate if the accepted risks can be further mitigated by relatively low cost measures. Furthermore they should maintain a register of accepted risks in order to monitor and re-evaluate the accepted risks over time. The risks might increase over time as the strength of cryptography deteriorates over time due to increased computing power. For example, users' passwords hash might have been stored in the past using the SHA-1 algorithm at the service provider. Although NIST already deprecated the algorithm in 2011, research published by Google in 2017 demonstrated a SHA-1 collision, i.e. two different files producing the same hash value[43].
4. Risk sharing – With this treatment the consequences of a risk is distributed with other parties. An manufacturer and service providers could collaborate in a partnership to share the risks. Risk transfer is a specific type of risk sharing in which the financial consequences of a risk are transferred on an insurance company.

Figure 7 shows the conceptual privacy risk matrix that combines the IoT vulnerabilities, the levels of personal data and the risk treatment options. Although the lines in this matrix are given pretty sharp between the different risk treatments, in practice these lines are grey areas. The type of treatment for privacy risks on the edge of an area should be assessed in a detailed risk analysis that takes all threats, vulnerabilities and mitigating controls into consideration.

Critical vulnerabilities combined with PII, sensitive, or special data should be avoided at all times. An example of a critical privacy risk that should have been avoided is the casus of security surveillance cameras in a sauna’s dressing rooms. The cameras got hacked in 2015 (critical vulnerability) and the camera footage of naked people (sensitive data) was captured by hackers[44]. While the cameras were removed immediately after the owner was informed, the recordings were still online on Internet forums in March 2018 [45].

The modification or risk reduction is the large section in the middle of the matrix. Manufacturers and service providers could consider to transfer the risk which is could make sense if highly sensitive data or special data according to the GDPR is collected stored and processed. The financial consequences of a

privacy data breach in these areas can be very high. The insurance company will require high security standards from the insurer to minimize the likelihood of a claim as part of their underwriting process.

From a privacy risk perspective, there is no risk at all if no personal data is involved. However, from an information security perspective, it is not desirable to bring a device with critical or high risk vulnerabilities on the market.

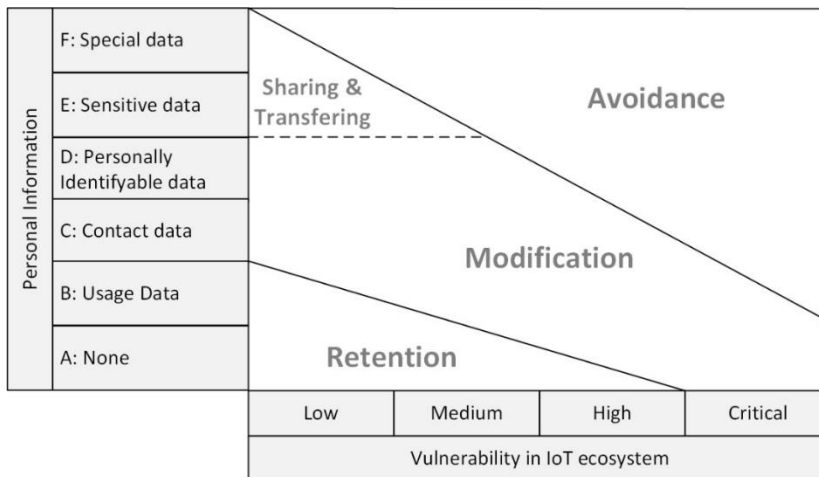


Figure 7: The privacy risk matrix with the risk treatment options for an IoT ecosystem.

## 2.5 Summary

Privacy risk is the risk of undesired disclosure of information about humans that materializes as a consequence of an information security incident. In turn, the likelihood of security incidents increases when the used technology, management and security processes, and the people’s behaviour in the IoT ecosystem have weaknesses that can be exploited. The privacy risk is driven by the combination of these vulnerabilities and the sensitivity of the personal information that is processed. The conceptual privacy risk matrix can be used to get a high level insight in privacy risks for an IoT solution. The security testers and researchers within various organizations can use this model to assess the information security and privacy risk as input for the

### 3 The design of the Security and Privacy Label

Traditional privacy policies of manufacturers and service providers provide insight in the service provider's intentions regarding the personal data that is being collected, processed and shared. This gives the user some insight in the potential impact of a security breach. The likelihood of a security breach is often unknown and can hardly be assessed by the user as it depends mostly on the effectiveness of security measures throughout the IoTs eco-system. Manufacturers and service providers on the other hand do have a better insight on the effectiveness of the security measures and therefore more insight in the likelihood of a security breach. Reducing this information asymmetry between consumers, manufacturers, and service providers is one of the main goals of the security and privacy label. *Labels can reduce uncertainty and overcome information asymmetry, but in order to do so, they need to present consumers with a meaningful reduction of complexity*[46].

A reduction of complexity is created by abstraction and leads to the loss of detailed information, meaning that a very simple label might not give enough information for consumers to compare two similar products quickly and easily. The information on the security and privacy label should therefore be balanced between simplicity and a complex model based on thorough lists of features and options. The most important criteria is that consumers should be able to compare similar IoT systems regarding the privacy risks that come with the use of the product. Requirements set forward by the Dutch Cyber Security Council include *"a labelling system (e.g. stickers on the packaging) to provide customers with information about:*

1. *the level of security of the device concerned;*
2. *if the device can receive automatic security updates;*
3. *the period during which the supplier will maintain the product;*
4. *if the device can be disconnected without loss of 'normal' functionality."*[14]

Other requirements regarding the labelling system are derived from literature research and the case studies described in chapter 5, 6 and 7 of this thesis [47][48][49]. The IoT privacy label should bring transparency by providing:

- Easy accessible and comprehensible information for consumers.
- Insight what personal information is collected and stored.
- Insight in where and by what organizations the data is processed and stored.
- Clarity about the data that shared with others.
- The choices given to the customer to in opt-in and opt-out regarding the collection and sharing of the data.

The approach that was taken in the design of the IoT privacy label was by starting and evaluating a privacy label based on the EU Energy label, because its relative simple format and the familiarity to the European citizens. The limitations of this simple privacy label were resolved by expanding the label with results of studies on privacy labels for web sites proposed by Reeder and Kelley. Their proposed models were adapted specifically for IoT systems while keeping the main approach to present the complex relationships between types of personal data, the purpose and recipients.

#### 3.1 The privacy label based on the EU energy label

The starting point for the design of a privacy label is the European energy label. The European energy label provides a simple design that is used to inform citizens about the energy efficiency of products, including household equipment, cars and buildings. The EU's main objective with this classification and labelling system is to inform the customers about the product's energy consumption so they choose to buy goods that consumes less energy and saves their money<sup>6</sup>. At the time of introduction it gave an

---

<sup>6</sup> <https://ec.europa.eu/energy/en/topics/energy-efficiency/energy-efficient-products>

incentive for manufacturers to produce more energy efficient products. The main component of the European energy label is the classification from A to G, where A (green) is the most efficient and G (red) the least. Figure 8 below shows the simple privacy label derived from the EU energy label combined with the six levels of personal information defined in table 2.

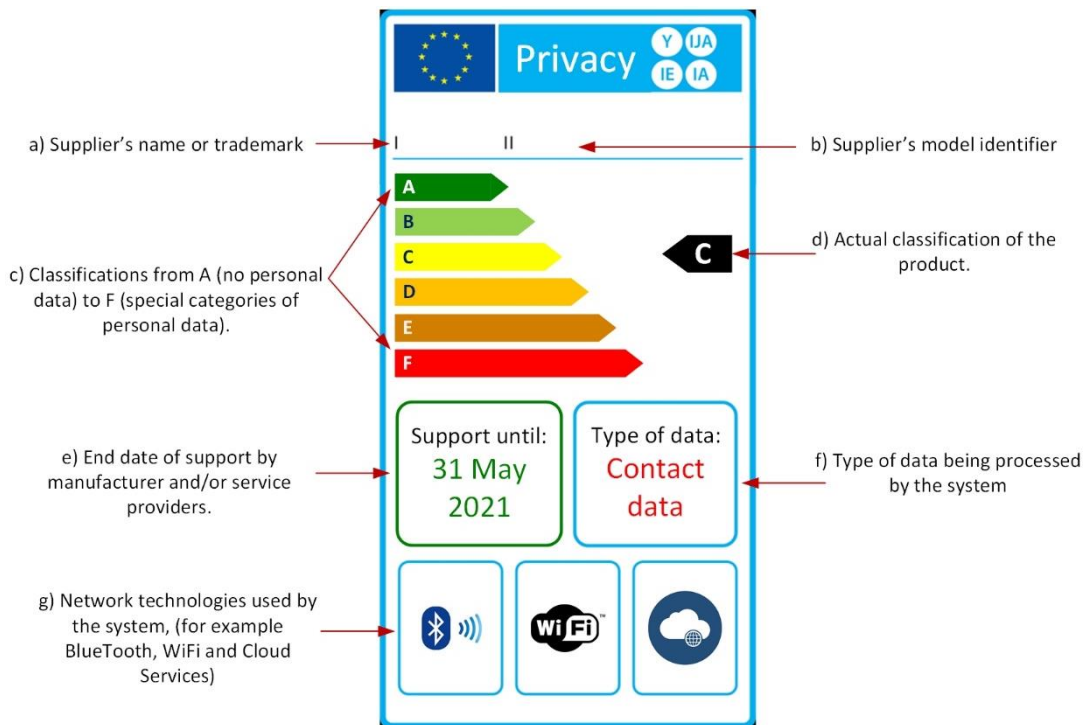


Figure 8: The simple privacy label based on EU Energy label.

Customers can quickly compare the labels of similar products and take the classification and the remaining support period in the decision making process. Furthermore, the information on the label is relatively static for the entire lifecycle of the product. The manufacturer and service suppliers should be committed and if necessary enforced through legislation and regulations to support the product and provide security patches until the end-of-support date.

The distinguishability between similar products is limited with the simple privacy label. Similar products are likely to process the same level of personal information and would be therefore be classified equally. Different manufacturers of lighting systems – that qualify as an IoT system – will most likely process a similar level of personal information, e.g. usage and contact information. There is no need to for a lighting system to ask for and process personally identifiable information or even more sensitive data (category D or higher). Comparing an alarm system that includes one or more surveillance cameras will automatically classify as a category E.

Another disadvantage is that the label only provides insight in the most sensitivity personal data that is being processed by the IoT ecosystem. It does not include what less sensitive information is collected and the information that is provided in the product’s usage policy or privacy policy. Information such as with whom the data is shared, and the opt-in and opt-out options are not provided in this simple label. Neither does the label provide insight in the level of security of the IoT ecosystem, i.e. insight in the likelihood about the leakage or loss of the personal data.

### 3.2 Reeder’s Expandable Grid model of the P3P standard.

The manufacturer and service supplier’s usage and privacy policies are not reflected in the simple privacy label, while they are quite relevant for a consumer. However, bringing the privacy policies to consumers

in an understandable manner is difficult because policies are presented or documented in various ways, which makes it difficult to compare them. In 2002 the Platform for Privacy Preferences (P3P) was created by the World Wide Web Consortium (W3C) with the objective “to enable websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents” [47]. P3P provides a standard XML format that websites could use to encode their privacy policies without the need of special server software. On the users’ side, a P3P user agent had to be implemented in the browser, which was the main problem for broad adoption. Further development of the standard was postponed after the publication of the W3C P3P 1.1 specification in 2006, due to the insufficient support by browsers.

The studies related to the P3P model and the lessons learned provide valuable input for an IoT privacy label. Reeder introduced the expandable grid for displaying privacy policies to Web users [48]. An example of this expandable grid is shown the figure below.

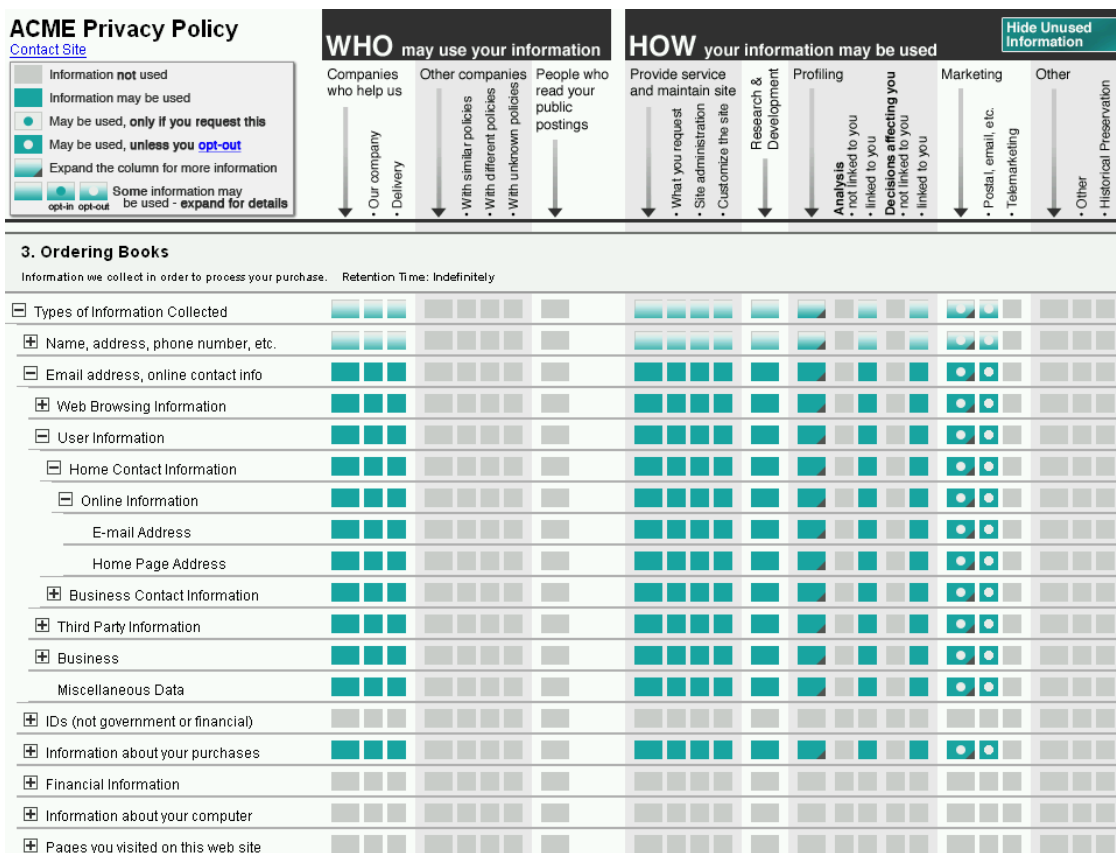


Figure 9: Example of P3P expandable grid for displaying privacy policies[48].

The expandable grid model visualizes a P3P policy based on the data structures in the P3P model. The P3P 1.1 standard has two hierarchies of data, which are built upon:

1. Categories – 17 types of information that companies can collect and includes types such as: Physical Contact Information, Online Contact Information, Unique Identifiers, Purchase Information, Financial Information, Computer Information and Navigation Information. These categories are given in the rows of the expandable grid model.
2. The base data scheme – contains each element or data type that can be specified in the P3P standard. These 89 defined elements are hierarchical arranged. For example the high level element User Data is the parent element of Name, gender, job title, home-info and business-info. In turn these elements have child elements, for example the element name has the elements: prefix, given middle, family, suffix and nickname [47].

Data elements can be a member of more than one category. For example name and its sub-elements can be part of the categories Physical Contact Information, Demographic and Socioeconomic Data. *“This led to nearly 800 elements per category (if fully expanded)”*[49].

The P3P data categories, purposes, and recipients are used as labels on the axis of the model. The purpose and recipient elements are placed on the horizontal axis, categorized in Who and How. On the intersection of each row (type of information) and column (recipient or a purpose) a variety of symbols and colors that represent the actual policy. The results of research on the expandable grid model strongly suggests that the model described above is not an effective means for presenting privacy policies. *“Participants using the Grid performed no better and no faster in correctly answering comprehension questions than participants using natural language. Moreover, subjective satisfaction scores show participants strongly disliked the Grid”*[48]. Further studies identified 5 major problems with the expandable grid model[49].

- *“Many of the P3P labels are not clear to users. For example, “Profiling” and “Miscellaneous Data” are not terms that users encounter in the context of their use of websites.*
- *The legend has a large number of symbols including multiple symbols for expansion (depending on directionality), which the user may not understand.*
- *Multiple statements that may be related to the same types of information in a P3P policy are displayed separately, possibly requiring the user to check multiple rows to answer a single question.*
- *The Hide Used Information button in the top right only condenses unused rows, not columns.*
- *Rows with a plus symbol may be expanded; however, many users (40.7%) never expanded any data types. By not expanding data types, users never saw some important parts of the policy.”*

These shortcomings provided input for further refinement of the privacy label by Kelley.

### 3.3 Kelley’s proposed Privacy Nutrition Label

Through several iterations Kelley et al. came to a proposed privacy label that simplified the expandable grid and incorporated the several general principles from the nutrition labeling literature[49]. Furthermore, the design goals of the label were to provide a single page summary of a privacy policy that *“improved the ability to find information, the understanding that there are differences between privacy policies and control over one’s information, and the simple time-based costs or reading privacy policies”*[49].

The final proposed model proposed by Kelley still uses the P3P concepts of data, purpose and recipient. However, the number of categories, purposes, recipients and symbols have been reduced strongly.

Important design features for this proposed Privacy Nutrition label are:

- The expandability was taken out of the data categories, only 10 main data categories are given in the model, one row for each data category.
- The short labels used for the column and row headers.
- The sub-elements of the purposes and recipients are removed, which reduced the number of columns. A description of the row and column header was handed out in an separate Useful Terms page describing the categories, purpose and recipients.
- Information that is not collected is also explicitly indicated.
- The row and column locations are consistent for the model, allowing for easy and fast visually comparison of different products.
- A legend that provides information about the meaning of each symbol.

## The Acme Policy

types of information	how we use your information					who we share your information with	
	provide service & maintain site	research & development	marketing	telemarketing	profiling	other companies	public forums
contact information	!	!	OUT	OUT	☐	IN	☐
cookies	!	!	OUT	OUT	☐	IN	☐
demographic information	☐	☐	☐	☐	☐	☐	☐
financial information	☐	☐	☐	☐	☐	☐	☐
health information	☐	☐	☐	☐	☐	☐	☐
preferences	!	!	OUT	OUT	☐	IN	!
purchasing information	!	!	OUT	OUT	☐	IN	☐
social security number & govt ID	!	☐	☐	☐	☐	☐	☐
your activity on this site	!	!	OUT	OUT	☐	IN	!
your location	☐	☐	☐	☐	☐	☐	☐

<b>understanding this privacy policy</b>	!	we will use your information in this way	☐	we will not collect or we will not use your information in this way
	OUT	we will use your information in this way unless you opt-out	IN	we will not use your information in this way unless you opt-in

**contact us** call 1 888-888-8888  
www.acme.com

Figure 10: Kelley's proposed Privacy Nutrition Label to visualize a privacy policy for websites[49].

The results from user satisfaction questions in the usability studies showed that the The Privacy Nutrition label was rated more pleasurable, easier to find information in, and easier and more enjoyable to use than the traditional written natural language policies. Other observations were:

1. Confusing labels for some of the participants.
2. Insufficient understanding of the opt-in and opt-out symbols.

The Privacy Nutrition label was designed with privacy policies of Internet websites in mind and has significant improvements over the Expandable Grid model. It is, however not directly suitable as a privacy label for an IoT ecosystem where a website is only one of the components.

### 3.4 The IoT privacy label

An IoT eco-system is more complex than a website in terms of components and the responsibilities for these components. A privacy label for an IoT eco-system is therefore likely to be more complex than for a website when the same level of detail is required. In an IoT eco-system there are different locations where different levels of personal information are stored and processed . The Privacy Nutrition label

cannot accommodate this information in its current form and needs some adjustments while maintaining the design concepts of:

- Single page privacy label for the eco-system to make the labels of similar products side-by-side easily comparable.
- Detailed information is based on data category, purpose and recipient.
- One row per data category.
- Information that is not collected is explicitly indicated by a symbol.
- Clarity about the opt-in and opt-out possibilities

The IoT eco-system privacy label can be created by combining the strengths of the different privacy labels, design practices and requirements set by the stakeholders such as users and government. As shown in Figure 11, the proposed IoT privacy label contains 3 main sections:

1. Overview – The top section provides the high level information regarding the privacy and the security of the IoT eco-system. It is presented in a way that allows for easy comparison of similar products.
  - a. On the left of the overview section the Simple Privacy label – as discussed in 3.1 – is provided to give a first indication about the level of personal information that is processed.
  - b. Specific security aspects and the privacy risk assessment – as discussed in chapter two – are given in the middle. The 4 properties in the Security and Compliance Information section are derived from the requirements set by the Dutch Cyber Security Council [50]. The outcome of a privacy risk assessment is plotted in the Privacy Risk diagram. The diagram includes a date to provide an indication how recent the information is. It is likely that the privacy risk changes over time, as new vulnerabilities will be identified and fixed by the manufacturers. IoT eco-systems should therefore periodically be monitored or audited during their lifecycle so that customers can be informed on the actual privacy risks when using the system.
  - c. The organizations that are part of the service delivery in IoT eco-system are listed on the left of the overview. These are the organizations from which you cannot opt-in or opt-out. Furthermore, the specific name and model is provided for matching the product with the privacy label and the links for further and actual information. A specific URL is given to the new IoT security monitoring service as proposed by the Dutch Cyber Security Council[50]. The barcode could be used in combination with an mobile app to directly retrieve the actual security and privacy data from the EU IoT monitoring authority.
2. The details section – This section provides insight on what personal information is processed, where it is processed and/or stored, for what purpose it is collected, and with whom it is shared. The following adjustments were made to the Privacy Nutrition label to accommodate the specific requirements for personal data in an IOT eco-system:
  - a. Two columns were added to indicate where the personal data is processed and stored.
  - b. The columns Marketing and Tele-marketing were combined into one column Marketing.
  - c. The data categories Cookies and Preferences were replaced by Voice & Video recordings and Genetic or Biometric data.
  - d. De category “Your activities on this site” is replaced with Usage Data and the order of categories is more aligned with the personal data classification as described in table 2.
3. The symbols and description in the legend “Yes, No, Opt-Out, and Opt-In” are updated to make them more clear[49].
4. The notes section allows for specific comments or remarks when the Opt-Out and Opt-In options are used in the detailed section.



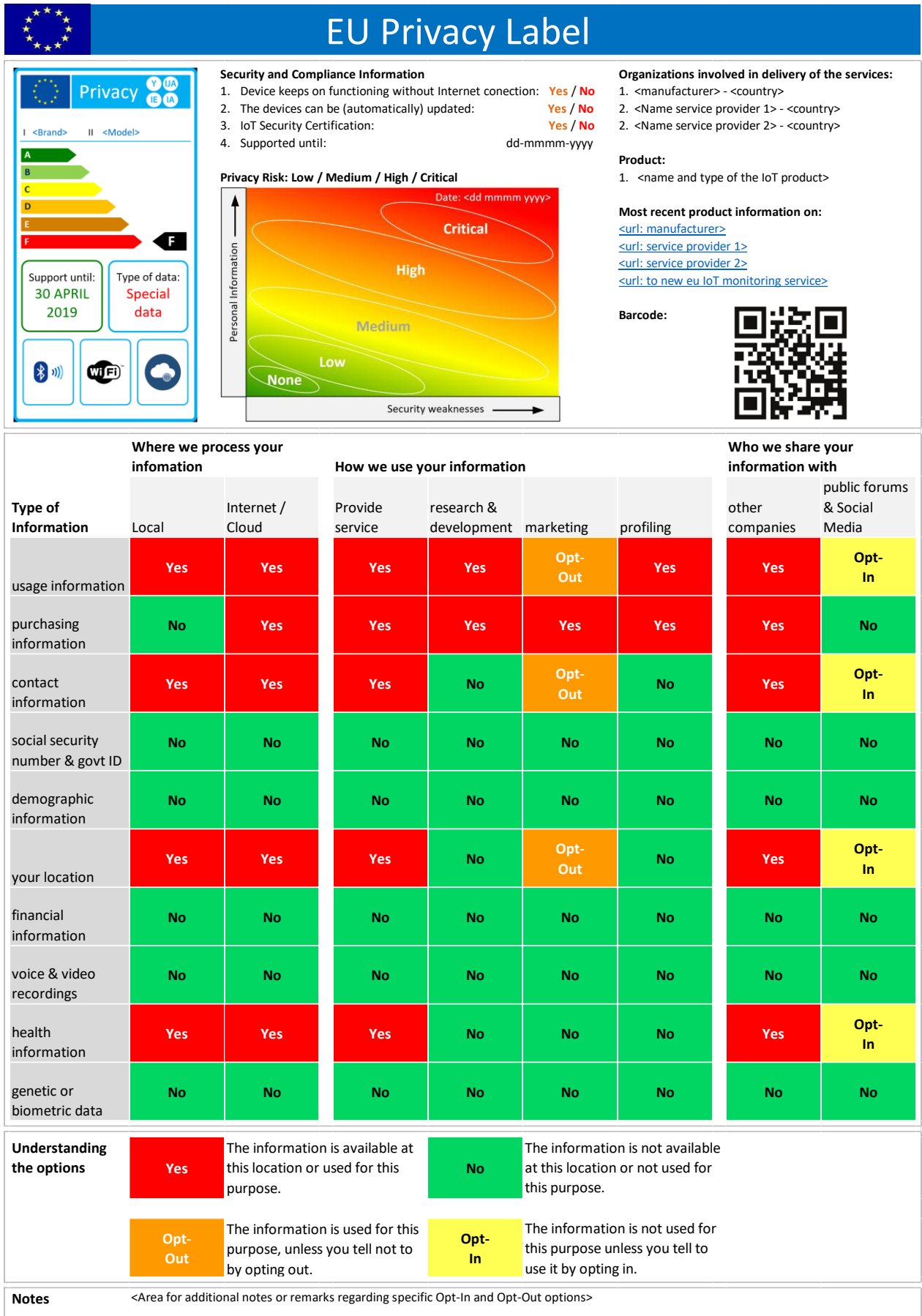


Figure 11: The IoT privacy label

While the IoT privacy label is designed as a single page, it can be difficult to put an A4 size sticker on the IoT product as required by the Dutch Cyber Security Council [14]. The design of the label gives the option to split the label into two parts and distribute the parts in different ways. The overview section can be printed and placed as a sticker on the packaging, while the detailed section can be accessed online through the URLs or the barcode. Especially an app on mobile devices could scan the barcode and retrieve the actual product information and details information while they are in the store.

The IoT privacy label given in figure 11 is just an example of a wearable that tracks the user's location, heartrate, sleep and daily activities. The information is uploaded to the Internet where other services are used to analyse the data and present the results to the user through webservers and mobile apps. The opt-in shows that the user can choose to share his data, including location and health related data with others. The label shows that besides the special data, also general personal data is shared such as usage, purchase, and contact information. The privacy label can show the differences between the many brands and types of wearables on the market.

Although the privacy label is designed for the consumer market, it could also be used in the professional medical solutions. For example Qualcomm Life's 2net platform is a professional eco-system that shares the user's biometric data from various devices and sensors with the doctors, caregivers, and family[51]. Similar to the consumer grade products, the professional system qualifies as a category F system because of the processing and storage of health related information. Health data is considered special data in the GDPR and defined as: "*Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject*"[34].

A description for each the elements in the details section of the label is given in the table below.

Table 3: IoT label elements [52][34]

Type	Element	Description
Where	Local	The data is processed and probably stored near the user, i.e. the layers 1 through 4 in the IoT Service model as described in the first paragraphs of chapter 4
	Internet / Cloud	The information is processed and stored outside the realm of the user, i.e. in cloud services, the layer 5 and 6 in the IoT Service Model.
Purpose	Provide service	The information is necessary to deliver the intended or requested services to the user by the system and service providers.
	Research & Development	Information may be used to enhance, evaluate, or otherwise review the service, product, or market. This does not include personal information used to tailor or modify the content to the specific individual nor information used to evaluate, target, profile or contact the individual.
	Marketing	The information is used to contact the user for the promotion of a product or service.
	Profiling	The information is used to determine the habits, interests, or other characteristics of the users in order to make predictions about and decisions that affect the user. For example by displaying ads based on the usage and purchase information of the product.
Recipient	Other companies	The information is shared with other companies in addition to the organizations named in the label's overview section. These organization are not directly involved in the operational service delivery but do have access to the data. For example tracking functions in the software that send information about the behaviour of a user to Facebook, while Facebook is not named as a primary organization in the IoT's eco-system[53].
	Public forums & Social Media	The information is shared with public forums or social media.
Type of information	Usage information	Information about how and when functionality throughout the IoT eco-system is used.
	Purchasing information	Information about the purchases made, including the payment methods.
	Contact Information	Name, address, phone-numbers

Type	Element	Description
	Social Security number & Government Identification	Government-issued identifiers such as social security numbers
	Demographic information	Information about social and economical categories that applies to the user, such as gender, age, and income.
	Your location	Information about the exact geographic location, often collected by GPS-enabled devices, including tracking devices, wearables and mobile phones and tablets.
	Financial information	Financial information such as accounts, balances, and transaction history
	Voice & Video recordings	Voice or video recordings from devices with microphones
	Health information	Information about the user's physical and mental condition including information about health care services.
	Genetic or biometric data	Genetic data is personal data that provides insight in the genetic characteristics which gives information about physiology or health of a person. Biometric data is personal data that allows for unique identification of a person, such as fingerprint and face recognition data.

### 3.5 Summary

This chapter described the design of an IoT eco-system privacy label based upon available models in literature and specific requirements from users, manufacturers and governments. The proposed IoT privacy label provides an overview and a details section on a single page that allows for easy and quick comparison of two products that provide similar functionality.

The type of personal data that is collected is likely to be stable. How this data is used and by whom is probably not really stable during the product's lifecycle as companies outsource more activities, merge with others or when the public becomes aware of specific undesirable practices. In addition, security measures in the IoT eco-system will deteriorate over time which increases the privacy risks. In order to provide customers with actual privacy risk information, the risk should be assessed periodically and also updated when new vulnerabilities are reported and resolved.

The following chapter describes the approach how the information required to populate the privacy label can be obtained.

## 4 Testing the components in an IoT ecosystem

An IoT ecosystem is built upon a mix of traditional technologies as well as new technologies specific designed for IoT devices, i.e. having low computing power and minimum power consumption. The conceptual six layer model given below is derived from two different four layer IoT models from Li and Scully and adapted by the experience from the case studies described in chapter 5,6 and 7 [54] [55]. The models from Li and Scully do not include the mobile devices or PCs that access the devices directly and/or the personal data through cloud applications at the service provider(s).

	<b>6. Cloud Application &amp; Services</b>	Specific cloud applications and back-end services to support the cloud applications, including storage, databases, device management, data analysis, and identity and access management services.	
	<b>5. Cloud Connection</b>	The Wide Area Network between the local network and cloud providers such as the Internet and mobile networks.	
	<b>4. Local Area Network</b>	Local Area Network (LAN), Wired and wireless ethernet including router connected to the Internet.	End-user devices PCs and mobile devices such as laptops, tablets and smart phones.
	<b>3. IoT Controller</b>	Gateways and (edge) routers and bridges to connect the device or sensor network to the Local Area Network (WiFi, IPv4, and IPv6)	
	<b>2. IoT network</b>	Zigbee, Z-wave, BlueTooth (LTE), WiFi, wired connections. (Personal Area Networks PAN)	
	<b>1. IoT Devices &amp; Sensors</b>	Toys, Light Bulbs, medical equipment, home automation, toys, wearables, etc.	

Figure 12: IoT Services Model

The shared responsibility for the users privacy is given on the left side of the model. The user has a large responsibility himself on the lower three layers and the manufacturers and service providers have more responsibility at the upper layers of the model. The conceptual six layers in the IoT services model can be described as follows:

1. The interaction between the physical world and the virtual or IT world takes place in the first layer where the physical devices and sensors are placed. The devices and sensors can record and process information related to their appliance. For example, the wearables measure heartrate, speed, and location that are synchronized periodically with other local systems (PC, phone or tablet) or directly to the cloud services. Alarm system sensors detect the position of a door or window (open or closed) and communicate this status periodically to the alarm gateway. Toys and personal assistants process voice recordings from the users and transmit these recordings towards the cloud services and submit the responses back through a speaker in the toy.
2. The IoT network layer provides the communication facilities for devices and sensors to communicate with their local IoT controller or gateway. Devices and sensors that use a WiFi connection can communicate directly with cloud services when connected to the local WiFi network on layer 4 (see figure 7 below). This direct connection is used by home-voice assistants from Google, Amazon and Apple and toys with similar functionality. The vast majority of IoT devices and sensors use a local wireless sensor network (WSN) based WiFi, Bluetooth, ZigBee, Z-wave or specific radio frequency (RF) to communicate with local IoT gateway.
3. At the IoT controller layer the IoT sensors are managed by a dedicated gateway and/or apps running on mobile devices that communicate directly with the devices. There are three main scenarios at this level as shown in figure 13:
  - a. A dedicated system, often called a bridge or gateway, is used to collect, store and process sensor and device information. For example the Philips Hue lighting system uses a bridge

for to send control messages to the individual lightbulbs over the ZigBee IoT network. The apps and web application (my.meethue.com) communicate with the bridge to control the lights. The gateway passes the status information to the cloud services. These architectures are used by the Philips Hue lighting system and the Egardia alarm system described in chapter 5 and 6.

- b. A standard PC, tablet or phone is used as a gateway. This architecture is used the toy “My friend Cayla”, described in chapter 7. For this reason, the PCs, tablets and phones are placed in the IoT device network layer. These systems can also act as workstation (control device) on any of the upper layers.
- c. The third type of controllers are the local workstations with a browser and mobile devices running an app that communicates directly to the gateway, which in turn controls the sensors. In this configuration there is no traffic on the local LAN. Alternatively, workstations running a browser connected to a different network than the gateway communicate with the gateway through the service provider. In this scenario, the bridge pushes its status to the cloud services frequently, which is pulled from the cloud service by the app. A change, for example turning on the alarm, in the app is transmitted to the cloud service. The gateway polls the cloud service every 30 seconds for updates and applies the change.

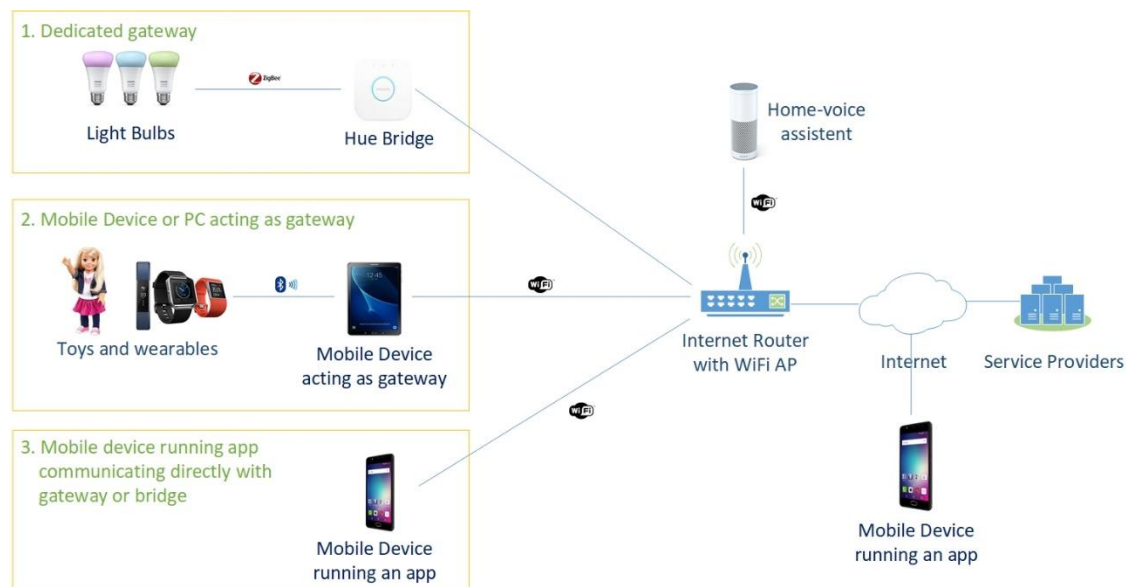


Figure 13: Various ways in which controllers are connected

4. The local network layer is the typical wired ethernet network and/or WiFi networks in houses. These local networks are connected to the Internet by means of a bridge or router. The IoT gateways and bridges use these local networks to communicate to local PCs and mobile devices as well as services on the Internet.
5. The cloud connection layer is the Internet and other wireless communication facilities such as the mobile telephone networks 3G and 4G. In the consumer market, it provides access to the cloud services for the local devices as well as mobile devices connected to mobile networks or different local area networks. Wireless metropolitan area networks (WirelessMAN) such as IEEE 802.16 or WiMAX and Long Range Radio (LoRa) are rarely used in the consumer market.
6. The cloud application layer provides a variety of web applications and services. Generally the Hypertext Transfer Protocol (HTTP) or the secure version HTTPS is used to transport data across the cloud connection layer to the cloud services. Security functions such as identification, authentication and authorization are very important at this layer to prevent unauthorized access and data leakage. An exploited vulnerability at this layer would potentially disclose personal

information of a large number of users. In case of a security breach it is important to have security logging and monitoring in place to assess the damage and inform the users and authorities about the disclosure or loss of the data. End-users should have insight where the applications and services are running and who has access to what data.

#### 4.1 IoT Architecture

As discussed in previous chapters, the IoT architecture is based on a distributed environment where the intelligence and provisioning of services is provided at the edge of the network, i.e. near the source of the data. This reduces the required bandwidth between the sensors and the cloud service and also reduces the power consumption at the sensors by using optimized net. In a smart home where a large number of sensors including cameras produce a considerable amount of data. In order to reduce the amount of data transported to the Internet and more importantly for privacy protection this data should be processed and stored as a first option [56]. Furthermore by having a local unit to process data provides the dependency on the Internet and cloud services reduces so that basic functions of the IoT solution are still available to the user.

The IoT ecosystem and its 6 layer model is presented in the figure 14 below with actual components and common symbols to make the model more tangible. Common types of devices, sensors, network and services are given in each layer. From a privacy protection perspective, the IoT devices and sensors process data that could be identified as personal, or personal information could be derived from it. It is likely that nobody is home when it freezes and the thermostat is at 15 degrees for the whole day. Higher in the stack the data is enriched by other data sources, for example the location data from the cell phones of the persons living in the house. When the location of all registered phones is “not at home”, the thermostat might automatically be turned to a lower temperature or the air-conditioning can be turned off. These relations between the whereabouts and the required action of the IoT device (temperature, lights, etc) is made in cloud application layer. By combining and analysing data from different IoT devices the personal information and knowledge can be obtained. An adversary that is after personal information on a large scale is likely to go after the data that is stored in the cloud. Access, however to the data in the cloud could be obtained by exploiting vulnerabilities on the lower levels. Security measures for the cloud applications and services should assessed in the same way as regular cloud applications such as email, social networks, and storage of personal files and photos.

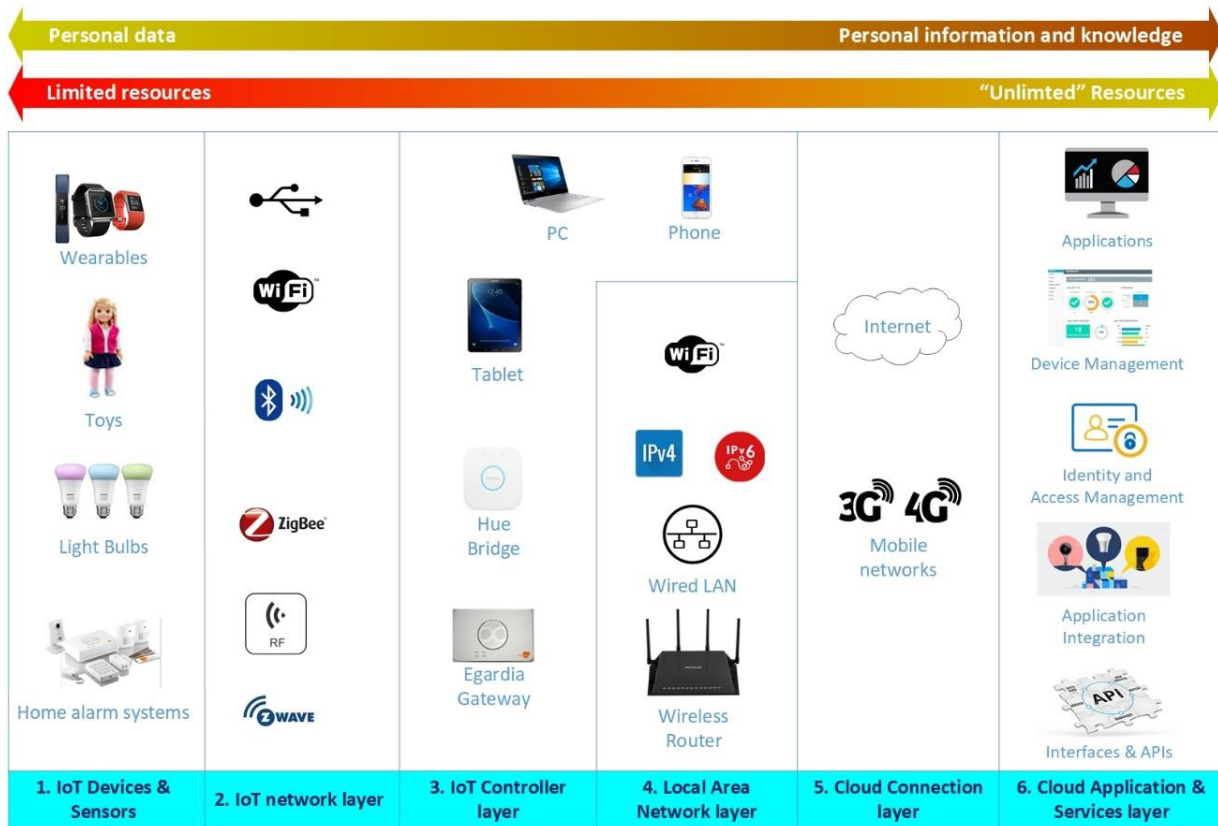


Figure 14: Attack vectors in the IoT ecosystem

The cloud layers generally have much more resources in terms of cpu, memory and power capacity compared to the lower layers. Especially the sensors running on batteries are very limited in resources and power consumption is kept to a minimum to use the batteries as long as possible. A consequence of these limited resources and the responsibility of the user to install and maintain the lower levels it is likely that the lower layers are more vulnerable to attacks than the upper layers.

The lower levels are likely to be attacked by adversaries who want to target individual persons or households, for example to:

- Spy, annoy or harass people, for example by eavesdropping on a private surveillance camera or just turning lights on and off in the house.
- Get into direct contact with children by exploiting vulnerabilities in toys.

The cloud applications and services are the target for adversaries who want steal large volumes of personal data or get control over a large number of IoT systems. Once in control of the local IoT system, the adversary can use these devices – with high speed internet connections – in botnets. Subsequently these botnets can be deployed for other attacks, including distributed denial-of-service (DDoS) attacks, sending spam, track victims connections and steal their credentials[57]. One of the first successful botnets targeted at IoT devices was the LizardStresser in 2016 [58]. This botnet was using default credentials for webcams or surveillance cameras, capable of generating 400Gbps of traffic[59]. Several DDoS attacks later in 2016 showed the rapid increase of capacity, generating up to 1.5Tbps of traffic from over 100.000 devices [58]. These large scale attacks were targeted at service providers, gaming sides, financial, and governmental institutions. Although these attacks cause havoc in society, the DDoS attacks are not a direct threat to an individual’s privacy because these attacks focus on the disruption of services and not on the disclosure of personal information. The DDoS attacks could also be used for distraction of the actual attack to steal personal data.

Adversaries can target devices and services in each layer of the IoT service model. Therefore each layer requires some form of authentication, authorization, logging, monitoring and cryptography. Especially weak configuration or the absence of these services could lead to leakage of personal data without being detected. For a privacy assessment of an IoT solution, each layer needs to be investigated.

The following general type of attacks can be launched from any of the 6 layers in the IoT service model. The consequences for each of these attacks is highly dependent on the type and amount of personal data that is processed at the compromised system or layer [60] [61].

- Eavesdropping or Man-in-the-Middle – Sniffing network traffic with the objective to abstract personal information or system information for subsequent attacks are most likely and easiest on the local wireless networks. Eavesdropping at the cloud connection, application and services layers is possible but would require an insider at the service provider or a compromised system at a service provider.
- Node Capture – an active adversary could try to extract privacy information from any of the devices in the ecosystem.
- Remote Control - Adversaries can try to obtain control over the device. Different types of attacks are possible to gain (partly) control over the IoT eco system. A replay attack is an example to gain control over a part of the IoT system.
- Rogue Gateway – The open structure and standards, diversity and weak security services allow adversaries to deploy their own gateways or take control over an existing gateway. A typical example is to take over an Bluetooth device that pairs automatically with any other system in the neighbourhood. This type of attack has the same outcome as the eavesdropping and controlling threats.
- Connected Device Denial of Service – These type of attacks can be launched by adversaries on each layer of the IoT service Model. These attacks will exhaust the resources at a particular level causing the system to fail. Wireless networks can be jammed so that communication in the system is hampered. This type of attack does not directly leads to the disclosure of privacy information but can be used to exhaust resources on the network so that it falls back to a lower level of security, for example a MAC flooding attack to be able to intercept network traffic from a switch [62].

The following paragraphs provide specific risks for each of the layers and how the security measures to protect the user's privacy can be tested and assessed.

## 4.2 The IoT physical device and sensor layer

The physical device and sensor layer forms the actual bridge between the real world and the digital or virtual world. The device or sensors in this layer receive actual data (temperature, sound, motion, GPS location, camera footage) from its environment. It converts these analog data into digital data and transmit it to other systems through the IoT device network layer for further processing and storage.

The level of personal information stored or processed on the device can range from close to none to very high in case the device has a microphone and/or camera. A smart thermostat might provide indirectly a little bit of personal data, i.e. a low temperature set on the thermostat low in the winter would indicate that probably nobody is home. The devices such as thermostats and wearables only process a limited amount of data that can be stored for a long period, which in turn can be used for profiling a person, family or household.

Devices such as a Surveillance camera, a personal assistant or a smart toy processes sensitive data. It is however not likely that the data is stored on the device. Beside the potential personal information, the device could also contain hard coded encryption keys used for secure communication with other devices and controllers in the IoT device network layer or local network layer. A defence strategy could be the



tamper-proof packaging or the implementation of a tamper reaction such as erasing all program or cryptographic memory [63].

#### **Risk**

Data stored on and processed by a sensor can be used for profiling a person or family. Cameras and voice recording devices can be used as a spy in a house. Retrieving information from a device or sensor itself, requires physical access to the device, which reduces the likelihood of unauthorized disclosure.

#### **Testing and Assessing**

It is important to understand what type of information is stored on the device. A physical inspection of the device could reveal the device is tamper proof. For all wireless devices there is an inherent risk of replay attacks, for example opening a smart lock on a door.

### **4.3 The IoT device network layer**

The IoT device network layer contains a network component and some sort of controller or gateway. The network component is often a wireless network, also called the wireless sensor network (WSN). The devices and sensors use this network communicate with other devices or gateways through a:

1. Wired connection, for example by a USB connection. Medical devices, toys and wearables may use these types of connection for updating the device and/or retrieving data from the device that was collected by the device over a period of time.
2. Wireless connection, which are used more often than the wired connections. A variety of protocols and standards are used to for these type of networks, including regular WiFi and Blue Tooth classic networks, as well as ZigBee and Z-wave networks that are specifically designed for these type of networks. ZigBee, Z-wave and BT-LE have low power consumption allowing the devices to run on regular batteries for a long time, up to 2 years in motion detection sensors . Finally other standards such as M-bus and proprietary protocols can be used on public radio frequencies 433 and 868 Mhz [64]. The following table shows an overview of the different characteristics of the different wireless protocols [65].

#### **Risk**

As with all communication networks, adversaries can eavesdrop on the network traffic and extract confidential information. Especially the wireless connections can be used by adversaries to eavesdrop on network traffic and to attack the devices and sensors with the objective to retrieve confidential information from these device or take control over these devices. The risk increases when a security device such as a smart lock or in-house camera can be attacked directly from this IoT network. Furthermore wireless networks are vulnerable for jamming attacks. Such a Denial-of-Service (DoS) attack reduces the availability of the system, but does not directly lead to the loss of confidential information.

#### **Testing and Assessing**

An important test is to verify that network traffic is encrypted to avoid eavesdropping on sensitive data. Furthermore this layer can be used to attack the sensors, devices and systems connected to the IoT network. Standards such as ZigBee, Bluetooth and WiFi have defined how authentication should take place. The strength of authentication should therefore be tested. Network analyzers and security testing tools are important gear to test the security on this layer.

Reported vulnerabilities of a product should be retested to verify if the vulnerability is adequately mitigated by the manufacturer. Furthermore weaknesses in one product caused by a weak standard are likely to be present in other products that use the same technology.

#### 4.4 IoT controller layer

The main components in this layer are the IoT gateway and the apps running on mobile devices. IoT gateways are more or less black boxes to the users. However, in practice, they are computing devices running a complete embedded version of Linux as operating system. The main difference from a regular Linux pc is that there is no screen and keyboard attached to the system. Hardening of the system is the responsibility of the manufacturer because the user has only limited or no possibilities to secure the system. Similar for the apps on mobile devices, the user is responsible for the security of the mobile device but the manufacturer for the security of the app itself and its distribution.

General security guidelines regarding system hardening therefore apply for manufacturers of IoT gateways. While hardening guidelines for Linux systems are publicly available on the Internet, the most basic ones such as using strong passwords for embedded accounts and disabling services that are not needed are often overlooked.

Manufacturers should provide updates in a secure manner, i.e. firmware updates should be signed by the developer and verified by the device to avoid implementation of compromised firmware, i.e. firmware with malware or backdoors.

##### Risks

The different type of devices in this layer leads to several applicable risks:

- The IoT devices and gateway have vulnerable services exposed to the local networks.
- Adversaries obtain full control of the IoT system due to weak authentication and authorization mechanisms.
- The deployment of compromised firmware is not undetected, caused by the weak distribution procedures and the lack of malware protection on IoT devices and gateways.
- Data leakage from mobile app caused by weak encryption of data at rest and data in transit.
- Data leakage caused by extracting confidential data and key material from the gateway through UART and JTAG interfaces. This risk increases if master keys and credentials of root accounts are used by all systems using the same firmware [66].

##### Testing and assessing:

Assessing the security of the firmware and its distribution mechanism requires the collaboration of the developer who can provide access to the firmware as well to the firmware distribution mechanisms. See also paragraph 4.6 on testing and assessing cloud services. In case the firmware file is available, tools such as binwalk can be used to decompose binary firmware files allowing the inspection of the actual embedded Linux system.

The mobile apps should be tested against the OWASP top 10 for mobile apps[67][68]. Vulnerability scanning tools such as Tenable's Nessus and nmap can be used to identify vulnerabilities of the IoT devices and gateways. These scanners will reveal open ports and vulnerable services.

#### 4.5 Local network layer

Home networks – wired and wireless – are often deployed and maintained by the users themselves. The networks are generally a flat IP network without any network segregation and firewalls between the networks. If an adversary has access to the wired or wireless network, he or she has direct access to all devices connected to the network. I.e. an adversary that gained access to the wireless network is able to eavesdrop on network traffic or attack the IoT systems directly. Access could be obtained in various ways, including a bad configured Internet router and poorly protected WiFi.

From an IoT privacy perspective, the inherent risks at the local network layer cannot be reflected directly on a security or privacy rating of the IoT system. The required security measures to protect against threats

on the local network should be implemented at the IoT controller layer and the cloud application layer. The strengths and weaknesses of security measures can be expressed in risk levels and reflected in a rating.

### Testing and Assessing

Monitoring the behaviour and communication paths of the IoT devices and apps is an essential test to assess the risk of data leakage by eavesdropping on network traffic on the local network as well as traffic to and from the cloud services. Network traffic analysers such as WireShark are necessary to investigate the IoT traffic.

## 4.6 Cloud connection layer

The cloud connection layer is provided by Internet providers and Telephone companies (Telco's) providing mobile Internet connectivity through their 3G and 4G networks. In the end, all data is transported over the Internet and this layer should be classified as insecure. Meaning that all data transmitted over the Internet should be adequately encrypted.

The risks on the Internet cannot be attributed to the IoT system directly. The cloud applications and services however should provide enough security measures to protect against the threats from the Internet. Risks caused by weaknesses in these security measure can be attributed directly to the IoT solution and influence the privacy rating.

### Testing and Assessing

The strength of the encryption can be tested in several steps on the local network. The first step is to identify the connections between the local IoT system and the cloud services. The next step is to inspect the communication between the systems on encryption levels. An Internet tool called Shodan can be used to find IoT devices that directly exposed to the Internet as well as insecure cloud services[69].

## 4.7 Cloud application and services layer

The cloud application and services layer collect, process and store the data from the sensors and enrich the data to information by integrating the collected data from different sources, including social media. Typical applications and services provided by the service providers are: application development, device management, data management, analytics and monitoring management [71].

Identity and access management is also part of the cloud services. Multiple standards exist for authentication, including username/passwords, multifactor authentication and identity federation. An industry standards for authorizations OAuth, which attempts to provide a standard way of providing access to services by means of an API without forcing the users to expose their credentials[72].

### Risk

Information security at the service providers is very important as they are an attractive target for adversaries who want to steal personal data on a large scale. The privacy risk for a user increases dramatically if the (main) service provider shares the information with other providers.

Accountability in case of data leakage can become problematic if there is no insight with whom and the conditions the data is shared. Within Europe, the user's rights are protected by the GDPR that became effective on 25 May 2018.

The two most important high level risks on this layer are:

- The cloud applications and or services contain vulnerabilities that can be exploited by an adversary. Successful attacks on web applications of service providers are in the news on a daily base.

- The services provider uses 3<sup>rd</sup> party services and shares sensitive information with this 3<sup>rd</sup> party without asking the user's consent or even inform the user about the sharing of information.

### Testing and Assessing

The cloud applications and services should be at least tested on the OWASP top 10 for web applications[70]. A substantial part of the testing on the OWASP top 10 vulnerabilities include penetration testing of web applications and services which require an explicit upfront approval from the service provider or owner. Getting the authorization to perform penetration tests get more complicated when the applications and services are hosted by a separate hosting provider. A possible solution could be mandatory assessments. These assessments or audits could be organized in various ways, through industry self-regulation and self-assessment or certification by an independent certification bodies similar to the ISO certification process[73].

An alternative approach is that the service providers in the IoT chain have their processes and systems audited by external auditors to attest the adequacy and maturity of the processes. Especially the Service Organization Control (SOC) 2 or SOC 3 Report could be useful in this situation[74]. A SOC 2 report is based on 5 trust service principles: Security, Availability, Processing Integrity, Confidentiality and Privacy[75]. A few pitfalls with the use of these reports are that the service provider can determine which trust principles are audited and for which systems and processes. A SOC 2 report from a service provider does not necessarily means that the privacy principle was part of the audit or that the report covers the systems and processes used to support the specific IoT system.

Examples of tests that can be performed in the lab are:

- Testing the strength of the encryption by inspecting the SSL/TLS certificates used by the service provider to encrypt the data to and from the service provider.
- Inspecting the SSL/TLS traffic with MitM tooling such as Burp or MITMproxy in a lab environment might provide insight in what systems and (versions of) software used in the back-end.
- Checking the effectiveness of the password policy.
- Review and assessment of the supplier's privacy policy.
- Search on the Internet on security incidents and complaints about the supplier.
- Use reconnaissance tooling such as Maltego to identify relationships of the supplier with other organizations.

## 4.8 Summary

The conceptual six layer IoT service model helps to understand the architecture of an IoT ecosystem and provides input for a risk based security testing approach. The security of the lower layers can be tested in a lab environment with the right equipment. Active penetration testing of the Cloud Application and Services layer requires the collaboration and approval of the supplier but there are tests and inspections that can be performed on the lab.

Specific risks have been defined for each of the layers but not all risks can be attributed directly to the security and privacy rating of an IoT product. For example: the manufacturer and service suppliers are not responsible for the vulnerabilities on the Local Area Network (LAN). The could however design the product robust enough so that can be used safely in an insecure network.

The IoT service model is used as the base structure in the three case studies that are described in the following chapters.

## 5 Case study 1: Philips Hue lighting

The Philips Hue offers a wireless lighting systems that allows the users to change the brightness and colour of the LED lamps, light strips and bulbs with HUE controls and mobile devices. Hue has four main components: the bridge, lights, the apps, and the portal. The core of the system is the “bridge” allowing the lights and controls to communicate with each other over ZigBee and remote control via the apps and the portal. The bridge offers APIs in a RESTful interface over HTTP (JSON) that allow for full control of the lights in the system, meaning a predefined set of stateless operations [76]. The apps are installed on mobile devices (iOS and Android to control the lights. The lights are the output of the systems that form a ZigBee mesh network with each other which enables each light to pass on messages to the next.

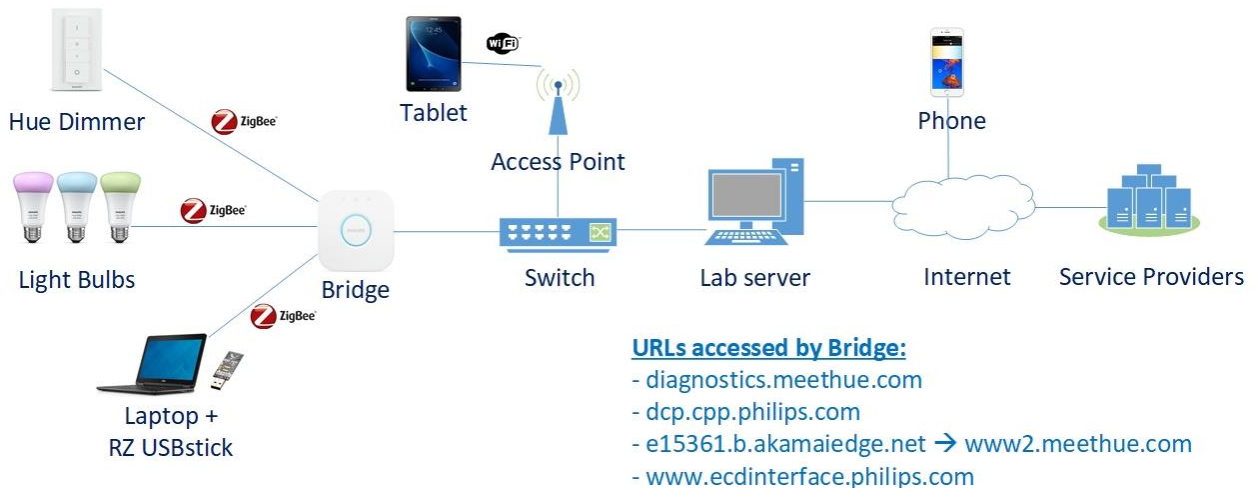


Figure 15: The lab environment for the Philips Hue lighting system

The security tests and the results for each of the 6 layers in the IoT services model are described in the following paragraphs. The final paragraph in this chapter provides an overview of findings and a risk assessment of these findings regarding the security of the system and the privacy of the user.

### 5.1 Layer 1: The light bulbs and dimmer

The Hue light bulbs and dimmer were not physically investigated or attacked in this experiment as they contain hardly any personal information. Most important information that the bulbs and control devices (switches, dimmers, and motion detectors) contain at this layer in the Hue system are the hard coded encryption keys, e.g. the ZLL master key. Obtaining the ZLL master key was not performed in this experiment because it would require to physically break a bulb while the key is already leaked on the Internet, and retrieving the status and/or controlling the light can easier be achieved on the ZigBee network as described in paragraph 5.2.

#### CVSS Score and privacy risk:

CVSS Base Score:	4.6		
Impact Subscore:	3.7		
Exploitability Subscore:	0.5		
CVSS Temporal Score:	4.5		
CVSS Environmental Score:	NA		
Modified Impact Subscore:	NA		
Overall CVSS Score:	<b>4.5</b>		
		<b>Security Risk</b>	<b>Personal Information</b>
		<b>Medium (4.5)</b>	<b>B: Usage data</b>
			<b>Privacy Risk</b>
			<b>Low</b>

<https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:P/AC:H/PR:N/UI:N/S:C/C/L/I:L/A:L/E:H/RL:U/RC:R>

## Conclusion

The security risks related the bulbs in terms of hardware hacking are limited and the bulbs themselves do not contain any personal information.

## 5.2 Layer 2: The ZigBee network

The IoT network layer in the Hue system is based upon a ZigBee network. Eavesdropping on ZigBee traffic was established by using Atmel's RZ Raven USB stick with special with specific firmware to support packet injection. This USB stick with the Killerbee software allows ZigBee network traffic to be analysed in WireShark[77].



```

▶ Frame 344: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
▶ IEEE 802.15.4 Data, Dst: 0xbbe7, Src: 0xb5c6
▼ ZigBee Network Layer Data, Dst: 0xbbe7, Src: 0xb5c6
  ▶ Frame Control Field: 0x0008, Frame Type: Data, Discover Route: Suppress Data
    Destination: 0xbbe7
    Source: 0xb5c6
    Radius: 1
    Sequence Number: 205
    [Extended Source: PhilipsL_01:01:a7:b5:0d (00:17:88:01:01:a7:b5:0d)]
    [Origin: 3]
  ▼ ZigBee Application Support Layer Command
    ▶ Frame Control Field: Command (0x21)
      Counter: 13
    ▼ ZigBee Security Header
      ▼ Security Control Field: 0x30, Key Id: Key-Transport Key, Extended Nonce
        ...1 0... = Key Id: Key-Transport Key (0x2)
        ..1. .... = Extended Nonce: True
        Frame Counter: 196609
        Extended Source: PhilipsL_01:01:a7:b5:0d (00:17:88:01:01:a7:b5:0d)
        Message Integrity Code: 53625717
      ▶ [Expert Info (Warning/Undecoded): Encrypted Payload]
    ▼ Data (35 bytes)
      Data: 1528cb42aa0dccc788741e38a6a0086807a33ffa8b5dc8458...
      [Length: 35]
  
```

Figure 16: Capturing ZigBee network traffic with the ATMELE RZUSBSTICK, Killerbee software and WireShark.

Several weaknesses of ZigBee Light Link (ZLL) and touchlink commissioning have been reported and demonstrated [78] [79]. Touchlink commissioning is besides the EZ-Mode commissioning a procedure introduced in the ZLL standard to link bulbs and control devices to a particular bridge[80]. Especially the recent research by Morgner et al. showed that the Philips Hue ZigBee implementation is vulnerable for different Denial-of-Service (DoS) attacks and attacks to gain control over the system[81]. One of the root causes of these vulnerabilities is the weak implementation of key management. All ZigBee traffic is encrypted with the AES-CCM algorithm using an 128-bit network key. An inherent problem with symmetric encryption is the distribution of encryption keys. In the ZLL standard the transport of the network key is encrypted by the ZLL master key that is known to all certified devices. This key is also distributed to manufacturers of the certified ZigBee devices and protected by a Non-Disclosure Agreement[80]. Inevitable the ZLL master key could not be kept secret and was leaked in March 2015<sup>7</sup>. The reported attacks on ZLL include[78][81]:

- Scanning for active devices – Without the knowledge or possession of cryptographic keys, the network can be scanned for active devices.
- Identify action attack – One of the functions in the touchlink commissioning procedure is to identify a light bulb in an app. When activated an instruction is send to the light bulb to blink several times. A special instruction can be crafted that keeps the Philips bulb busy for 18 hours.
- Reset to factory default – This attacks resets the light bulb to factory default and therefore out of control for the legitimate user. The user can get control back by recommissioning the bulb to the bridge. This in turn provides the opportunity for the adversary to obtain the network key because of the weak network key distribution mechanism described above.
- Permanent disconnect attack – In this attack the bulb is reconfigured for a separate ZigBee channel and commissioned to a non-existing or the adversary's network. As a consequence the legitimate user cannot recommission the bulb from the regular apps.
- Hijack attack – In this attack the bulb is connected to the adversaries network, which gives the adversary full control over the bulb.

<sup>7</sup> Leakage of ZLL and OTA keys on <https://twitter.com/mayaZigBee?lang=nl>

- Network key extraction – Commissioning new bulbs or bulbs in factory-default state enforce the transmission of the network key encrypted by the leaked ZLL master key. The adversary can eavesdrop on the network traffic and intercept the exchange of the encrypted network key and subsequently decrypt it with the leaked ZLL master key.

To assess the actual vulnerabilities regarding privacy leakage two approaches can be taken:

1. Obtain information from the manufacturer. In case the assessment is performed in collaboration with the manufacturer, this should be the first step to obtain information what has been fixed and how. If there is no direct collaboration than the manufacturer’s release notes are an alternative source for information. Unfortunately, the Philips Hue bridge release notes are not informative at all. Only general descriptions are provided about the support of new devices and the general statement “*Stability and other performance improvements*” [82].
2. A replay of the network key extraction. This test failed in our lab environment, even after resetting the bridge and all light bulbs to factory default. The network key could not be decrypted by WireShark (see figure 16), while the leaked ZLL master key and Trusted Link Keys were configured in WireShark. A sample .pcap file from KillerBee revealed the network key without a problem. Possible reasons for the failed test are:
  - a) The wrong procedure was followed in resetting the recommissioning the light bulbs.
  - b) The Hue system uses new or different keys that have not yet been leaked.

The Z3sec software, used by Morgner et al in their investigations, could not be used because this software did not work with our available lab equipment, although the documentation of the Z3sec software states otherwise [83].

As a counter measure against the various attacks, the ZigBee specification recommends to minimize the the wireless range of touchlink commands. Meaning that devices should be in close proximity for touchlink commissioning, which is max 1,8 meter for the Hue bulbs [81]. However, Morgner et al were also able to launch identify action attacks from a distance of 36 meter and extract a network key from a distance of 130 meter.

### CVSS Score and privacy risk

CVSS Base Score:	5.8			
Impact Subscore:	3.7			
Exploitability Subscore:	1.6			
CVSS Temporal Score:	5.2			
Overall CVSS Score:	5.2			
		Security Risk	Personal Information	Privacy Risk
		Medium (5.2)	B: Usage data	Low
<a href="https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L/E:F/RL:O/RC:R">https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L/E:F/RL:O/RC:R</a>				

### Conclusion

The vulnerabilities that can be exploited on the ZigBee network are some form of DoS attack, i.e. the user has (temporary) no control over the lights. The damage can be recovered by the user but it is a cumbersome process. The security risks are therefore more related to the availability than the confidentiality of the bulbs and bridge, that do not process personal information. The privacy risks are therefore assessed as low.

### 5.3 Layer 3: The Hue Bridge and app on mobile devices

The Philips Hue bridge fulfils the role as IoT gateway and has a wired connection to the local network. The apps on mobile devices are used to control the light bulbs and can communicate directly with the bridge over the local network. Different tests are applied to these components.

### 5.3.1 Direct Communication between App and Bridge

The app on a mobile device has two communication paths to the bridge. If it is in the same LAN (IP network) then the app uses HTTP to communicate with the bridge. There is no encryption of data and the tokens can be retrieved directly from the http data in the packet as shown below. HTTPS is used through the cloud services when the mobile device is in a different IP network.

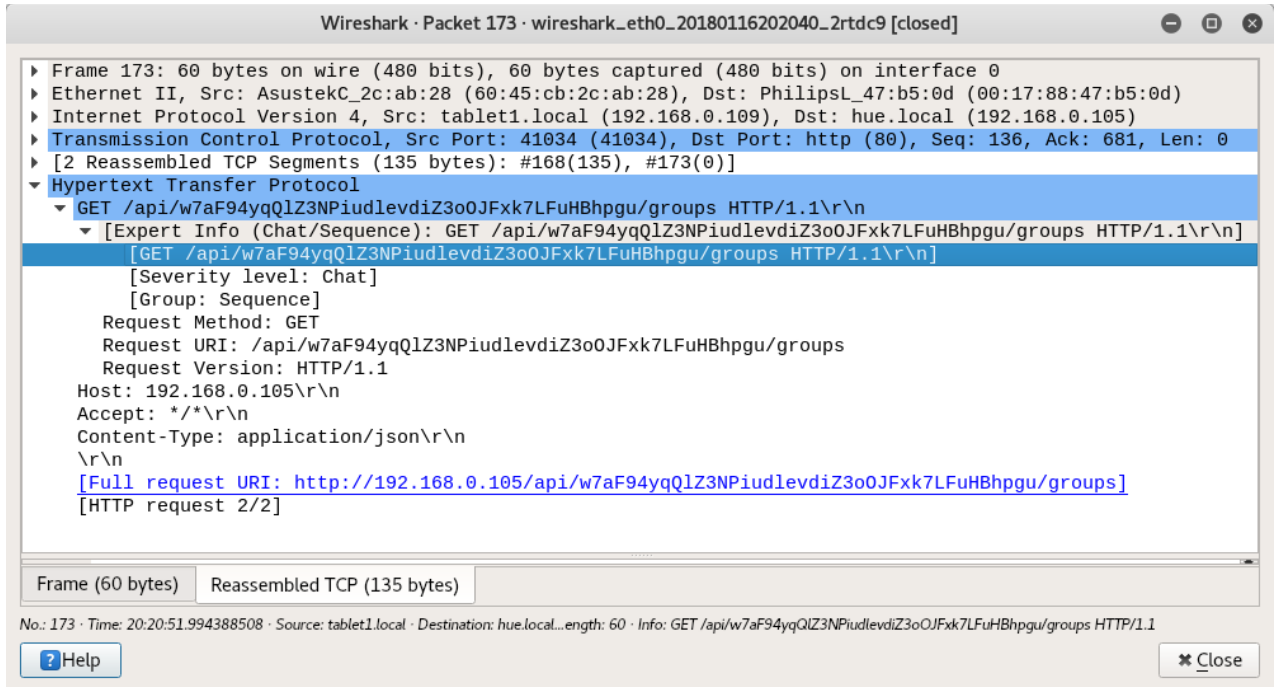


Figure 17: Bridge accounts are transmitted in clear text on the local network

### 5.3.2 Testing the Hue bridge

Devices such as the tablet register with the bridge by launching the app and after the bridge is found by the app, the button on the bridge needs to be pushed for acceptance. This means that physical access to the bridge is necessary to authorize an app. In the background the bridge creates what is called a “username” and places this on a whitelist. This “username” that is created at the bridge is actually a 40 character token that can be used for authentication to use the APIs on the bridge. Everybody in possession of such a username (token) can operate the lights and can also create new usernames through the APIs when there is access to HTTP on port 80 on the bridge. This is because there are no authorization mechanisms on the bridge and the APIs on bridge can be used to create new usernames and “press the button” remotely. There is no need to develop specific code, because the build-in CLIP API Debugger provides the necessary tool (see Appendix B for more details).

The list of authorized devices or token on the bridge is not aligned or synchronized with the authorized apps in the cloud at <https://account.meethue.com/apps>. In the situation as shown in figure 17, the first three accounts on the bridge, including a rogue device, are not shown on the list in the browser. Since the app on the Android device has no functionality to review or modify the list of accounts or tokens on the bridge, the user has no options to review or delete the accounts. The “Cleaning” option for the bridge in the app does not delete the usernames, i.e. a regular user is not able to disable or delete old usernames. The only way is to reset the bridge to factory default by pressing the pinhole button on the back of the bridge.



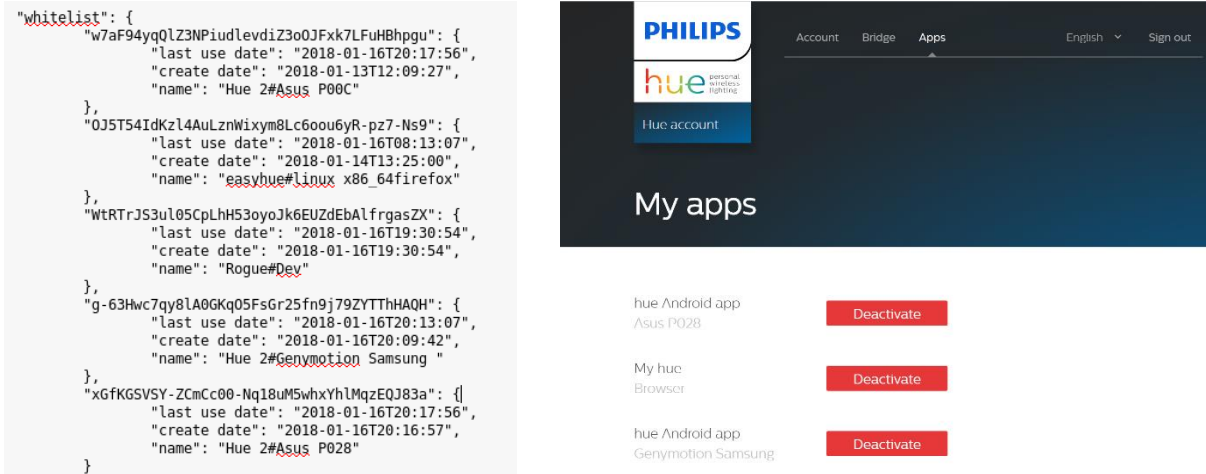


Figure 18: Accounts on the Bridge are not aligned with the authorized apps in the cloud services.

A scan with zenmap and Tenable’s vulnerability scanner Nessus showed that port 80 and 8080 are open. Where port 80 is the web services providing some static html pages and the Clip API debug tool.

Nmap Output	Ports / Hosts	Topology	Host Details	Scans																				
<table border="1"> <thead> <tr> <th>Port</th> <th>Protocol</th> <th>State</th> <th>Service</th> <th>Version</th> </tr> </thead> <tbody> <tr> <td>80</td> <td>tcp</td> <td>open</td> <td>http</td> <td>Philips Hue wireless lighting bridge</td> </tr> <tr> <td>4638</td> <td>tcp</td> <td>filtered</td> <td></td> <td></td> </tr> <tr> <td>8080</td> <td>tcp</td> <td>open</td> <td>http</td> <td>Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd</td> </tr> </tbody> </table>					Port	Protocol	State	Service	Version	80	tcp	open	http	Philips Hue wireless lighting bridge	4638	tcp	filtered			8080	tcp	open	http	Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd
Port	Protocol	State	Service	Version																				
80	tcp	open	http	Philips Hue wireless lighting bridge																				
4638	tcp	filtered																						
8080	tcp	open	http	Web-Based Enterprise Management CIM serverOpenPegasus WBEM httpd																				

Figure 19: Zenmap output of scan on Hue bride

While Zenmap identified a Web-Based Enterprise Management (WBEM) interface on port 8080, Nessus only identified the open port and found no specific vulnerabilities. A search on the Internet did not provide any hits on the WBEM management interface on the Hue bridge. It is likely that the port is enabled for troubleshooting and diagnostics but from a security perspective it would have been better to have it closed. This would avoid the risk that the port or service can be exploited in some way. The Hue bridge has a universal asynchronous receiver-transmitter (UART) port on its motherboard that can be used for diagnostics. It can also be misused to become root on the bridge[84]. More insight in the open port 8080 could be obtained in this way. This test however has not been done in this research.

### 5.3.3 Testing the Hue app for Android

The security of the App was tested by performing automated static code analysis of the app by three different products [28][29][30]. The tools Quixxi and Ostarlab are online services while MobSF is installed locally on a Windows laptop. The following table provides the summary of the output of the three different tools. Due to the absence of an Apple mobile device, the iOS version of the app was not tested.

Table 4: Code review of Philips Hue App v2.18.0 by different tools.

Tool	High risks	Medium Risks	Low risks	Rating
Quixxi	<ol style="list-style-type: none"> <li>File Unsafe Delete check</li> <li>Certificate Pinning</li> </ol>	<ol style="list-style-type: none"> <li>Outputting logs to logcat / logging sensitive information</li> </ol>	<ol style="list-style-type: none"> <li>Usage of installer verification code.</li> <li>Executing “Root” or system privilege check</li> <li>Unencrypted credentials in database</li> </ol>	<p>4.2 / 5</p> <p>Failed</p> <p>6 out of 34</p>
Ostarlab	none	<ol style="list-style-type: none"> <li>Application does not enforce binary protections (ASLR, NX, RELRO and Stack canaries)</li> </ol>	<ol style="list-style-type: none"> <li>4 exported activities accessible to other services.</li> <li>Retrieved source using open-source decompilers</li> </ol>	

Tool	High risks	Medium Risks	Low risks	Rating
MobSF	<ol style="list-style-type: none"> <li>1. Found ELF built without stack protection</li> <li>2. 4 activities are shared with other apps on the device.</li> <li>3. The app uses a weak hash code that should not be used in Secure Crypto.</li> <li>4. App uses SQLite DB and executes raw SQL queries, can cause SQL injection</li> <li>5. App uses insecure Random Number Generator</li> </ol>	none	<ol style="list-style-type: none"> <li>1. IP address disclosure</li> </ol>	NA

The three different tools found different issues and assessed the risks also quite different. Especially the MobSF tool rates potential issues as “High”. The four shared activities are created as “high severity” by MobSF, while they are mentioned as “Important” by Ostorlab. The actual risk of using a weak hash code and insecure random number generator should be further investigated. This investigation is, however, beyond the scope of this research. The MobSF framework also provides the option to perform a dynamic code scan of the app. Due to time constraints, this test has not yet been performed.

Quixxi provided a unique set of vulnerabilities and the reporting is more usable for this research. The main reported risks are that files are not deleted safely. Meaning, they can be recovered by any user or adversary, especially on rooted devices and the app does not have the code to check if the device is rooted. The certificate pinning request is confirmed by an MitM test in the lab with Portswigger’s tool Burp. The app stopped when an untrusted certificate was presented by Burp. After importing the Burp root certificate on the tablet, the app was able to authenticate and username and password could be intercepted. Decryption of the traffic to from the App to the cloud services revealed that the entire configuration from the bridge can be retrieved, including the tokens. The replay attacks can be performed as long as the session with the server is valid. After an idle time out of +/- 30 minutes, the session is terminated.

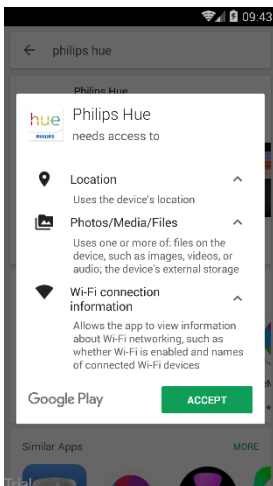


Figure 20: Required access of Philips Hue App on device.

The App requires access to the location, local files and WiFi connection information. It is not clear why the app needs access to the files. The location information and WiFi information is necessary for the “Home & Away” functionality which allows to turn off the lights when the device’s location is about 500 meter from the location market as “home”. When the device comes within a reach of 500 meter of the home location the assigned lightbulbs are turned on. During the investigation it was not possible to eavesdrop on the TLS traffic between the mobile device and the cloud service. The behaviour of the app on its location seems that it only sends a message to the cloud service once it crosses the 500 meter boundary, i.e. no data is send if the location changes and the device stays within or outside the 500 meter distance from the home location. Although the actual coordinates were not intercepted, the bridge maintains the location of the configured devices in terms of within reach or out of reach. This information can be retrieved through the Bridge APIs as shown in figure 43 in Appendix B.

The MitM test was only partly successful in eavesdropping on encrypted network traffic with Burp. The leaking of actual location information (GPS coordinates) to the cloud services could therefore not be inspected. The Philips Lighting privacy notice does not clarify this as it states “Location information – Your actual location (derived from your IP address or other location-based technologies), that may be collected when you enable location-based products or features such as through our apps.” [39].

**CVSS Score and privacy risk**

<b>CVSS Base Score:</b>	8.8	<b>Security Risk</b>	<b>Personal Information</b>	<b>Privacy Risk</b>
Impact Subscore:	5.9	<b>High (8.0)</b>	<b>C: Account Tokens and indication of location of device<sup>8</sup>.</b>	<b>Medium</b>
Exploitability Subscore:	2.8			
<b>CVSS Temporal Score:</b>	8.0			
<b>Overall CVSS Score:</b>	<b>8.0</b>			
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:R				

**Conclusion**

The app communicates in clear text with the bridge, including the authentication token. An adversary that captures such a token can have complete control over the bridge and subsequently the connected light bulbs. Furthermore the adversary can determine which devices that are configured for Home & Away functionality, are within a range of 500 meters to the Hue bridge.

The user has no insight what systems have access to the bridge and is not able to delete tokens from the bridge that no longer need access.

Parts of the Hue Android App and the Meethue web applications do not use certificate pinning. This makes the application vulnerable for MitM attacks when the user ignores the browser warnings or when an adversary has compromised the system and is able to install a rogue certificate on the mobile device. Information related to the device location could only be retrieved from the bridge, not by eavesdropping on communication between the device and the cloud services.

**5.4 Layer 4 and 5: the local network and cloud connection layers**

The security of the Local Area Network is an important aspect of the security for the Hue system. It is the user who is responsible for the security of this layer. Although the Internet Service Provider provided the Internet router, it is the customer that needs to change the default passwords and configure the wireless network.

A compromised LAN, wired or wireless, give adversaries access to the Hue bridge. One of the main success factors of the IoT botnets was the direct connection of the IoT devices to the Internet while still having the default admin username and password on surveillance cameras [57]. The router between the local network and the Internet should block network communication sessions that are initiated from on the Internet. Only sessions initiated on the local network are allowed to pass through the router. The Hue bridge has a web service running on port 80 that should only be accessible from the Internal network and not from the Internet.

A web application called Shodan can be used to identify wat systems and services are exposed directly on the Internet including the vulnerabilities. This tool can be also be used to find Hue bridges that can be accessed from the Internet. A search on Shodan (<https://maps.shodan.io>) with the title of the default Hue webpage reveals a number of bridges that are directly connected to the Internet, with the Netherlands ranking on the 4<sup>th</sup> place with 175 devices[69]. An adversary that wants to attack a single house could lure the owner with social engineering to press the button on the bridge, or find a way to obtain an existing username on the target bridge. This existing username can be used to access the API to “Press the Button” remotely.

<sup>8</sup> Through the debugging API an indication of the location of the device can be obtained. The indication is if the device is in the proximity of 500 meters from gateway. The coordinates of the gateway, i.e. the home location, are not registered.

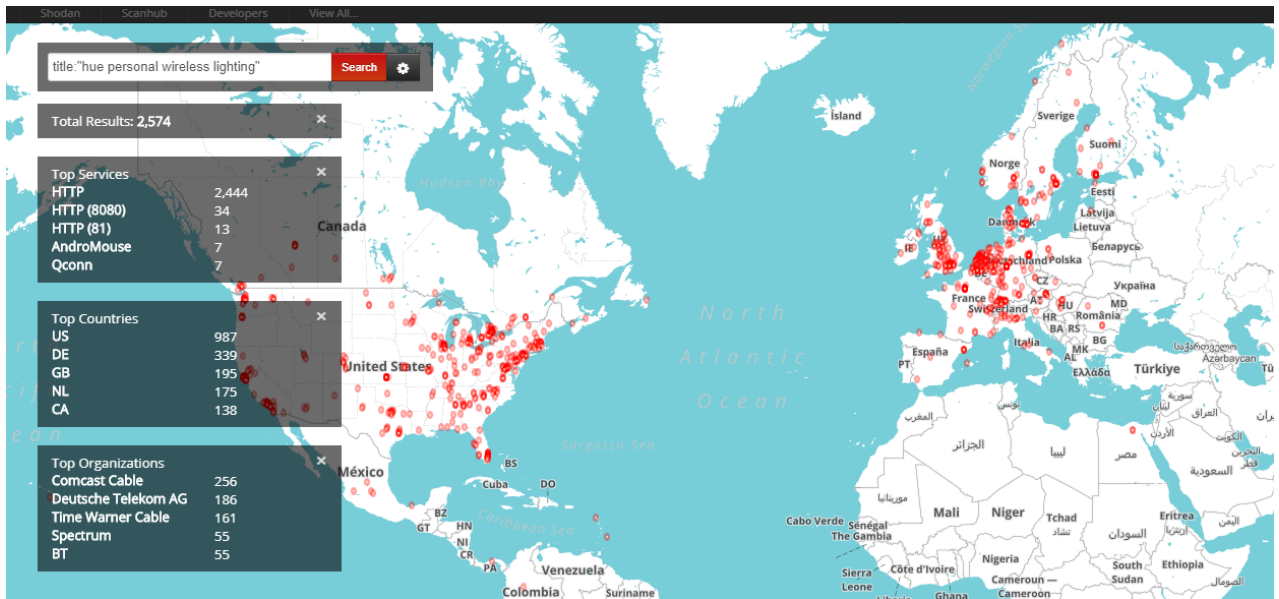


Figure 21: Hue bridges directly connected to the Internet [69]

Beside the threats from the Internet, a MitM attack on the local network can also be successful to gain access to the Hue bridge. In the lab, an MitM attack was performed from the wireless network while the bridge was connected by wire to the switch on the same IP network. By starting an ARP spoofing attack, all traffic from the bridge and workstations in the network were redirected to the workstation on the wireless network. By eavesdropping on the network traffic the account data could be obtained as shown in figure 17.

**Conclusion**

The local network layer and cloud connection layers are the most important layers used by adversaries. These layers are still useful in the 6 layer conceptual model to better understand the threats and risks related to the IoT controller layer and cloud application and services layer.

**5.5 Layer 6: Cloud application and services layer**

After installing the Hue bridge with the three light bulbs traffic to and from the bulb was monitored. In total of 37788 packets were captured in 24 hours. Analysis of the packets showed that the Hue bridge submits AES encrypted data to dcp.cpp.philips.com when the lights are turned on, off or dimmed and hourly if no changes occur. The graph below shows the packets transmitted do dcp.cpp.philips.com over 16,5 hours, when the lights were turned on/off/dimmed several times. The large spikes show a status change, the hourly small spikes (4 packets) show an hourly update cycle to the cloud service.

The Hue bridge communicates with several services on the Internet which are hosted at several service providers. Table 4 shows an overview of these services including the way data was encrypted and the SSL Server Rating Guide given by Qualys to that server[85].

Table 5: Cloud services communicating with the Hue Bridge

#	IP Address	DNS name	Hosting/Service provider	Encryption	Encryption Classification
1	5.79.62.93	dcp.cpp.philips.com	Rack Space	HTTP with AES	na
2	95.100.96.56	www2.meethue.com	Akamai Technologies	HTTPS	Qualys A
3	162.13.31.14	<a href="http://www.ecdinterface.philips.com">www.ecdinterface.philips.com</a>	Rack Space	HTTP with AES	na
4	130.211.93.93	bridge.meethue.com 93.93.211.130.bc.googleusercontent.com	Google	HTTP with AES?	na
5	104.155.18.91	ws.meethue.com 91.18.155.104.bc.googleusercontent.com	Google	TLS v1.2	Qualys T / B (due to name mismatch)

#	IP Address	DNS name	Hosting/Service provider	Encryption	Encryption Classification
6	130.211.67.12	diagnostics.meethue.com 12.67.211.130.bc.googleusercontent.com	Google	HTTP with AES?	Na
7	35.190.18.125	time.meethue.com 125.18.190.35.bc.googleusercontent.com	Google	HTTPS TLS v1.0	Qualys A

Note: the certificate for ws.meethue.com cannot be trusted due to a name mismatch. The trust that can be given to this encryption is seriously degraded. The app functioned without problems, this could indicate that the certificate for this service is not verified.

The bridge communicates for some processes in plain HTTP but the payload is encrypted with AES as shown in the figure below. Various parameters are used for authentication, replay prevention, etc. The effectiveness of these security measures were not further investigated.

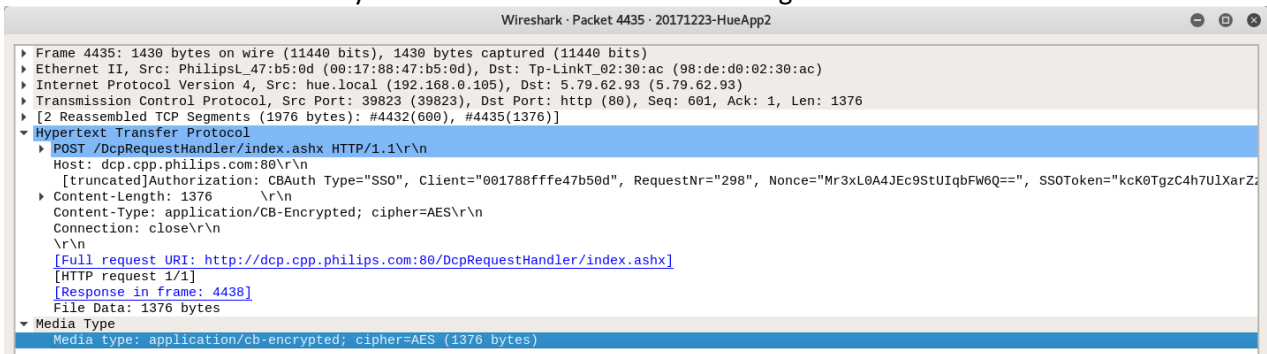


Figure 22: AES encrypted data in HTTP protocol

In order to use the cloud services an account has to be created by a browser on my.meethue.com. The registration process requires the following information:

- Username
- Email address
- Preferred language
- Country
- Password, no password complexity rules only a minimum of 8 characters. A google account could also be used as account for the could application my.meethue.com and account.hue.com

Since no other information is provided to the Hue ecosystem it classified according to table 2 as a privacy risk at level C (Contact Information). The Philips Lightning privacy notice is easy to read, but it does not provide the user and clarity in what data it shares with others. It states that various sorts of data is collected that it is: “not shared except in a limited number of cases” [39]. These cases are, however, described in a very broad way and include Philips-Lighting affiliates, service providers, business partners, public and governmental authorities, professional advisors and others, and other parties. The lack of clarity the privacy notice does not help in reducing the privacy risk of the user.

The following table shows the list of services that the app is connecting to. The app communicates directly to the bridge in HTTP when it has direct access, i.e. device and bridge are in same IP network segment. All communication between the app and the bridge go through the cloud services when the app and bridge are in different IP networks.

Table 6: Communication of the Hue app with cloud services

#	IP Address	DNS name	Hosting/Service provider	Encryption	Encryption Classification
1	52.213.23.109	api.meethue.com plb00hue-1843182927.eu-west-1.elb.amazonaws.com	Amazon	TLS v1.2	Qualys A

#	IP Address	DNS name	Hosting/Service provider	Encryption	Encryption Classification
2	130.211.12.238	account.meethue.com 238.12.211.130.bc.googleusercontent.com	Google	TLS v1.2	Qualys A+
3	66.117.29.226	philipslighting.dc3.sc.omtrdc.net (public html content)	Adobe systems	HTTP	na
4	74.6.105.9	agent.portal.flurry.vip.bf2.yahoo.com	Yahoo	TLS v.12	Qualys A
5	74.6.34.10	data.flurry.com	Yahoo	TLS v1.2	Qualys A

Inspection of the traffic to data.flurry.com showed specific information about the mobile device is sent to the provider, see appendix C for details.

### CVSS Score and privacy risk

CVSS Base Score:	5.8			
Impact Subscore:	3.7			
Exploitability Subscore:	1.6			
CVSS Temporal Score:	5.2			
Overall CVSS Score:	5.2			
		<b>Security Risk</b>	<b>Personal Information</b>	<b>Privacy Risk</b>
		<b>Medium (5.2)</b>	<b>C: Contact Information</b>	<b>Low</b>
<a href="https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:H/PR:N/UI:N/S:C/C/L:I/L/A:L/E:F/RL:O/RC:R">https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:H/PR:N/UI:N/S:C/C/L:I/L/A:L/E:F/RL:O/RC:R</a>				

### Conclusion

The communication with the cloud services from the bridge as well as the app are encrypted. All SSL/TLS certificates were good with the exception of ws.meethue.com. Which is assessed as a medium security risk. The privacy statement given by Philips does not provide any clarity for the user about wat data is shared with whom. Since the amount of personal information is limited to contact data, the privacy risk for this layer is assessed as low.

## 5.6 Summary of issues

The following table provides an overview of identified issues that the assessed risks for these issues. The amount of personal information is that is provided to Philips is limited, which reduces the privacy risks.

Table 7: Philips Hue overview of findings and privacy risk assessment

Layer	Findings	Security Risk	Personal Info	Privacy risk
1	No material deficiencies were identified	Low	A: None	Low
2	1. The ZigBee network can be used by adversaries to launch several DoS attacks on the bulbs and controllers	Medium	B: Usage	Low
	2. The bulbs can be hijacked and fully controlled by the adversary	Low	B: Usage	
	3. Network key can be extracted from eavesdropping on ZigBee network traffic.	Medium	B: Usage	
3	1. Network traffic between the app on the LAN communicates in clear text over HTTP, allowing the security token to be intercepted.	High	C: Account tokens and location indication	Medium
	2. The legitimate user has no insight in the actual applications/devices that have access to the Bridge.	Medium	B: None	
	3. Port 8080 is open the bridge with seems like a WBEM management interface. The open port and services are not documented – no reported vulnerabilities have been found in the Internet	Medium	Low <sup>9</sup>	
	4. The app and browser do not use certificate pinning, which makes them vulnerable for MitM attacks. Adversaries can fully	High	C: Account tokens and	

<sup>9</sup> The risk is assessed as low because there were no vulnerabilities found. This could however change rapidly if the port provides functionality that is not documented, i.e. security by obscurity which is not good.

Layer	Findings	Security Risk	Personal Info	Privacy risk
	control the bridge and retrieve location related information, e.g. determine if the mobile device with the app is at home or not.		location indication	
6	1. No transparency on what data is shared with partners. The amount of data is however limited to email address, country, and preferred language	Low	C: Contact Information	Low
	2. One certificate for ws.meethue.com has a name mismatch. The risk is assessed as medium because the data is still encrypted. The particular process using this service does not seem to check the certificate name.	Medium	C: Contact Information	Low

The table above shows that the Hue bridge and the app at layer 3 have the most security issues and consequently the biggest threat to the user’s privacy. Especially the unencrypted communication over the local network makes eavesdropping on local traffic and retrieving the user’s location related information from the bridge relatively easy.

The diagram below shows the identified issues in the privacy risk matrix and it shows the two medium privacy risks and 7 low risk issues. These issues could be resolved by encryption of the communication on the local network and applying certificate pinning to the Hue app.

Personal Information	F: Special data				
	E: Sensitive data				
	D: Personal Identification data				
	C: Contact data				
	B: Usage data		(2.1) (2.3) (3.2) (6.2)	(3.1) (3.4)	
	A: None	(2.2) (3.3) (6.1)			
		Low	Medium	High	Critical
Information security risk in IoT ecosystem					

Figure 23: Privacy risk matrix for Philips Hue system

### 5.7 The privacy label for the Philips Hue light system

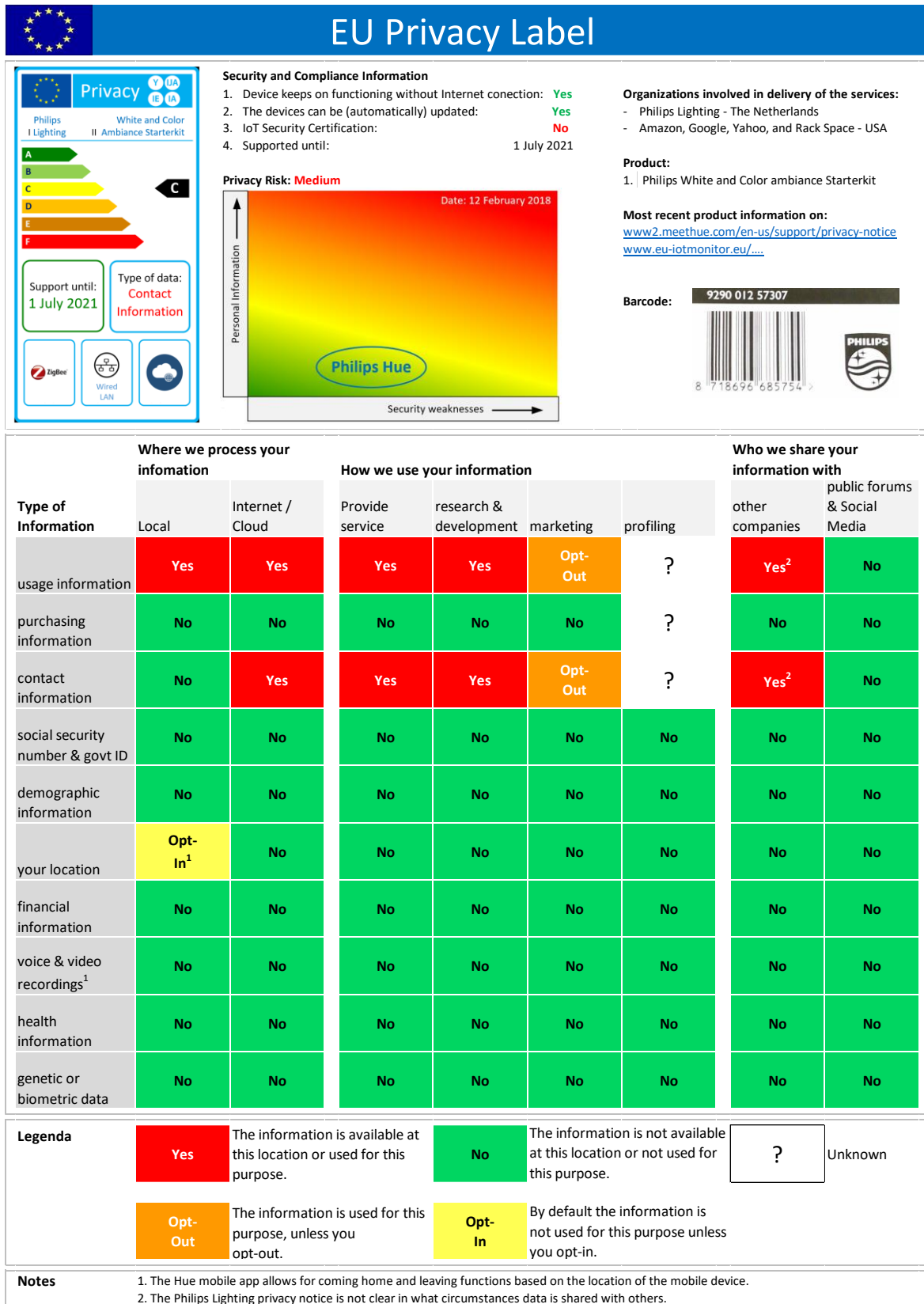


Figure 24: The IoT privacy label for the Philips Hue lighting system

Note: The “support until” date in the label overview is a fictional date and intended only as an example.



## 6 Case Study 2: The Egardia alarm system

The Egardia alarm system is available in Belgium, France and Germany. On the Dutch market it is sold with the brand name Woonveilig in major retail stores. The Egardia ecosystem is created by sensors and controllers, an alarm gateway, cloud applications and services, and apps for mobile devices. Different sensors such as motion, smoke, water and door opening detectors can be used to trigger an alarm. These events are received by the gateway that, when the system is armed, sets of the siren and sends the alarm message to the cloud services. In turn the cloud services send automated voice and text messages to the configured phone numbers. The web based cloud application has to be used to configure the alarm system. Egardia provides these cloud services through a subscription that costs €8,95 per month. An additional subscription is required when an Egardia surveillance camera is used with the alarm system.

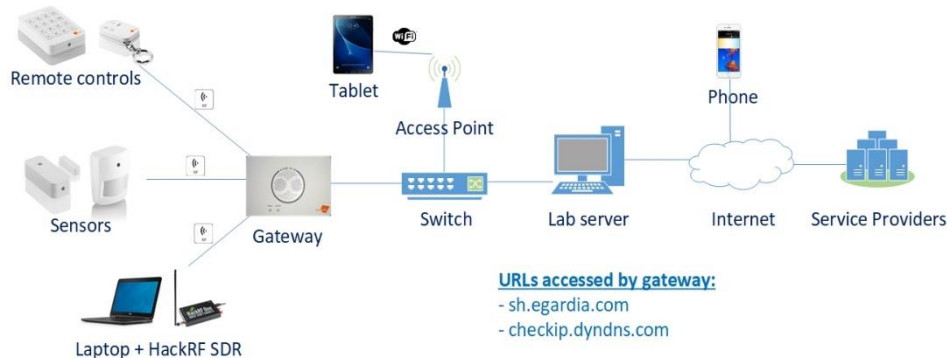


Figure 25: The lab environment to test the Egardia alarm system

The starter kit that was used in this research contained an Egardia gateway (type Gate-03), a keypad, a key fob, two motion detectors and a door/window sensor as shown in figure 25. A surveillance camera was not included in this starter kit.

All sensors and remote controls work wireless and use a frequency of 868 MHz without any specification of standards used for the communication between the sensors and gateway. Furthermore, no information is publicly available regarding the security measures build into the product. With the remote controls, the user can arm and disarm the alarm system. The manual states that configuration should be performed through the cloud services. Although not documented by Egardia, a fully functional web server on the gateway allows direct configuration and management of the gateway and sensors.

Information gathering on the Internet about the Egardia product revealed that Egardia is using the hardware from Climax Technology in Taiwan. Other alarm system brands using Climax Technology hardware include Blaupunkt and Lupus Electronics [86]. Reported vulnerabilities on these systems could also be applicable to the Egardia system because they all share the same core operating system on the gateway. Several issues were reported in July 2016 regarding the vulnerabilities regarding the Lupus alarm system[87]. They assessed the technical risk of the identified issues as “Critical” and the likelihood of exploitation as “Medium”.

Egardia also provides a service to connect surveillance cameras to the alarm system and allows the camera footage to be viewed on the App and through the web based app. This service supports four cameras and costs an additional €4,-- per month. This service and functionality has not been testing in this research. However, leakage of account information would provide an adversary also provide access to the video footage.

### 6.1 Layer 1: The alarm sensors and controllers

All sensors and remote controls such as the key pad and key fob are wireless devices powered by batteries. Each of these devices is paired with the gateway by pressing a button on the gateway to set in a discovery mode and then press the button on the sensor so that it will be discovered by the gateway.

The HackRF software defined radio (SDR) was used to monitor the RF signals at 868 Mhz. This monitoring tool showed that the sensors keep sending motion detection and door open/closed signals to the gateway

even if the alarm is turned off or disarmed. This could provide adversaries an indication that an operating alarm system is working, as indicated by the stickers on the outside doors and windows of the house. The peak in the spectrum diagram in figure 25 shows the signal sent by the motion detector. The transmissions shown in the bottom part of the diagram show the signals from the different sensors over a short period of time, by deliberately moving in front of the motion detector, opening and closing the door. These RF signals can be recorded and replayed as described in paragraph 6.2.

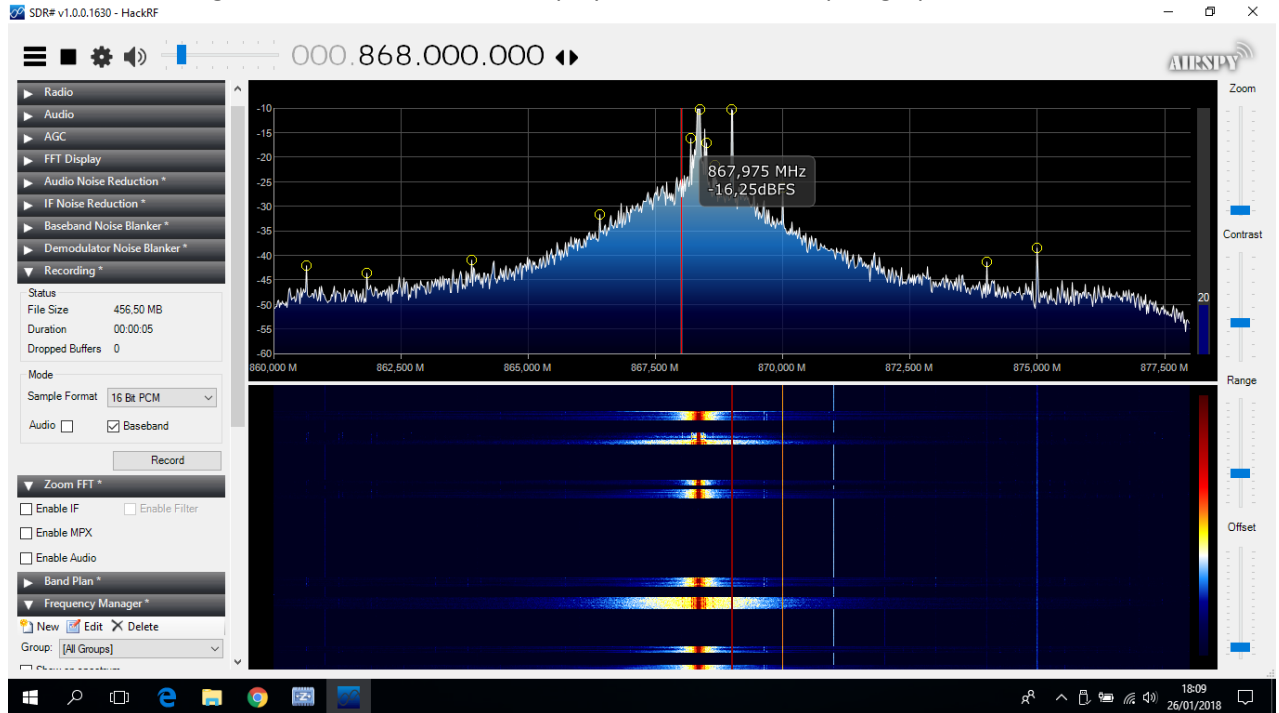


Figure 26: Spectrum analyser showing the RF signals send by sensors on 868 Mhz.

A physical inspection of the sensors and controls showed that the circuit boards in the sensors and controls can accommodate but have not installed tampering switches. The red circles in the picture below show where the components could be installed in the keypad, the motion sensor and door switch as shown in the picture below.

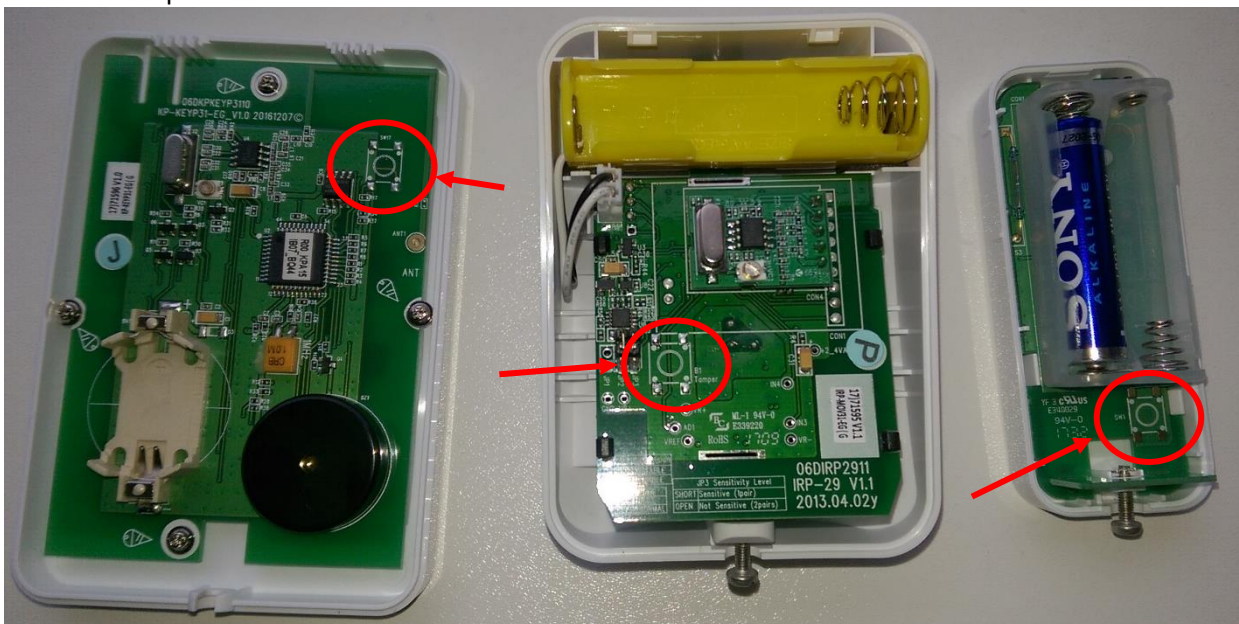


Figure 27: Missing tampering components in keypad, motion sensor and door switch.

**CVSS Score and privacy risk**

CVSS Base Score:	5.7	<table border="1"> <thead> <tr> <th>Security Risk</th> <th>Personal Information</th> <th>Privacy Risk</th> </tr> </thead> <tbody> <tr> <td>Medium (5.5)</td> <td>B: Usage data</td> <td>Low</td> </tr> </tbody> </table>	Security Risk	Personal Information	Privacy Risk	Medium (5.5)	B: Usage data	Low
Security Risk	Personal Information		Privacy Risk					
Medium (5.5)	B: Usage data		Low					
Impact Subscore:	4.7							
Exploitability Subscore:	0.9							
CVSS Temporal Score:	5.5							
Overall CVSS Score:	5.5							
<a href="https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H/E:H/RL:U/RC:R">https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H/E:H/RL:U/RC:R</a>								

**Conclusion**

The lack of tempering detection and the sensors of an alarm system is calculated as a medium security risk. Simply removing the battery from a sensor is noticed by the gateway after 36 hours. Once noticed, the gateway will triggering an alert that the sensor has lost connection. Another risk related to the behaviour of the sensors is that personal presence in the house is detectable in the proximity of the house due to the continuous operating mode of the sensors. This is still considered a low privacy risk because the amount of personal information is limited to usage data.

**6.2 Layer 2: The wireless sensor network**

Inherent vulnerabilities of wireless communication are jamming and replay attacks. Jamming the radio signal is a denial of service attack that can be detected but not prevented. Replay attacks can be prevented by using rolling code. The HackRF One tool can be used to successfully launch a replay attack. First the raw RF signals, sent by the key fob, to arm and disarm the alarm system were recorded by the Software Defined Radio (SDR). These signals could be replayed by the SDR, allowing an adversary to turn off the alarm system, enter and leave the house without triggering an alarm, and finally turn the alarm system back on. The logs of the alarm system will show that the key fob was used to turn off the alarm during the trespassing. The successful replay attack indicates that there are no effective measures implemented to prevent this type of attacks.

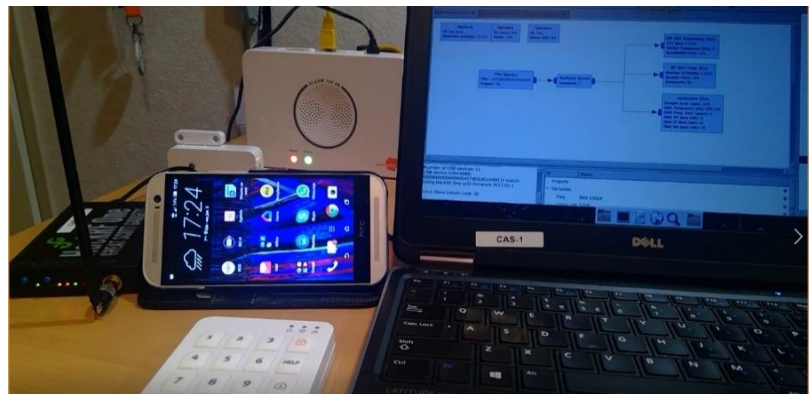


Figure 28: Using the HackRF One and GNU Radio Companion for replay attacks

Figure 28 shows the main components in this test: the laptop running the GNU Radio Companion, the HackRF One, the Egardia devices, and a mobile phone that receives the alarm text messages.

**CVSS Score and privacy risk**

CVSS Base Score:	7.8	<table border="1"> <thead> <tr> <th>Security Risk</th> <th>Personal Information</th> <th>Privacy Risk</th> </tr> </thead> <tbody> <tr> <td>Medium (6.8)</td> <td>B: Usage data</td> <td>Low</td> </tr> </tbody> </table>	Security Risk	Personal Information	Privacy Risk	Medium (6.8)	B: Usage data	Low
Security Risk	Personal Information		Privacy Risk					
Medium (6.8)	B: Usage data		Low					
Impact Subscore:	6.0							
Exploitability Subscore:	1.2							
CVSS Temporal Score:	6.8							
Overall CVSS Score:	6.8							
<a href="https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:H/PR:N/UI:R/S:C/C:L/I:H/A:H/E:P/RL:U/RC:U">https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:H/PR:N/UI:R/S:C/C:L/I:H/A:H/E:P/RL:U/RC:U</a>								

**Conclusion**

The weaknesses in the wireless sensor network between the sensors, controllers and gateways allow adversaries to disarm the complete alarm system, prevent sensors to trigger an alarm, or generate false alarms. Unauthorized disarming the alarm system is a medium to high risk from a security perspective. Personal information is hardly present at this layer and the privacy risk is therefore considered as low.

### 6.3 Layer 3: The alarm gateway

The primary function of the gateway is to receive the data from the sensors and controllers and trigger an alarm when the system is armed or partly armed. Another important function for the gateway is to fetch configuration changes and software updates from the cloud service. During the experiments an upgrade became available for the gateway. Egardia only provided release numbers without any further information on what has been changed or fixed in the new release.

#### 6.3.1 Communication between gateway and cloud services

The gateway communicates every 10 seconds with the cloud service to push and pull configuration information to and from the cloud service. For communication with the cloud service the gateway uses an unencrypted HTTP connection with base64 authentication. Decoding the authentication string showed that the username and an MD5 hash of the initial user's password is used that was set in the registration process of the alarm system. An adversary who is able to perform a MitM attack can take the MD5 hash and run it and try to crack the password offline. Once the password is cracked the username and password can be used to login to the cloud service and fully control the alarm system.

Users have to manage their account and configure their alarm system through the cloud service. Changes to the configuration and accounts, including password changes, are retrieved by the gateway in XML format with a ten second poll interval. Since the communication is HTTP, all changes are transmitted in clear text. This makes manipulation of the poll request and responses possible and allows the adversary to:

- Turn on and off the alarm remotely.
- Eavesdrop on the clear text password initiated by password changes in the cloud application.
- Set the password for the first system user that was obtained by decoding the base64 authentication header.

#### 6.3.2 Penetration testing on the Egardia gateway

An initial port scan with Zenmap shows that port 80 (http) and 55023 (BusyBox telnetd) are open. Neither of these services are described in Egardia manuals. The functionality of the web server is, however, described on similar alarm systems manufactured by Climax Technologies [88].


The web server running at port 80 provides access to the gateway's configuration. The public home page shows security related information such as internal and external IP addresses and firmware versions. All other pages from the menu require a username and password using basic authentication. The credentials used when registering the alarm system with the cloud services can be used to login to the web service embedded in the gateway. The menu options in the web service provide much more options in configuring and monitoring the alarm system. The vulnerability scanner Netsparker reported 2 high, 2 medium and 5 low vulnerability risks for the webservice running on the gateway. The high risk vulnerabilities are about the transmission of passwords and basic authentication information over HTTP, i.e. transmitting username and password in clear text over the network. An adversary who obtained the username and password of the system user, as described in previous paragraph, gets full control over the alarm gateway.

Since neither of the HTTP and telnet services are used in the Egardia ecosystem, these ports should be closed on the gateway. Hardening the gateway by closing the ports makes the system reduces the consequences of a successful MitM attack on the LAN and cloud connection layer.

#### 6.3.3 The Egardia App

The security of the App was tested by performing automated static code analysis of the app by three different products [28][29][30]. The following table provides the summary of the output of the three different tools. Due to the absence of an Apple mobile device, the iOS version of the app was not tested.

Table 8: Code review of the Egardia App v2.4.4 by different tools.

Tool	High risks	Medium Risks	Low risks	Rating
Quixxi	<ol style="list-style-type: none"> <li>1. SSL Implementation check – SSL certificate verification</li> <li>2. Fragment vulnerability</li> <li>3. File unsafe delete check</li> </ol>	<ol style="list-style-type: none"> <li>1. Outputting logs to logcat / logging sensitive information.</li> </ol>	<ol style="list-style-type: none"> <li>1. Usage of installer verification code</li> <li>2. Not performing a “Root” or privileged check.</li> <li>3. Unencrypted credentials in databases.</li> </ol>	4.0 / 5  Failed 7 out of 34
Ostorlab	None	<ol style="list-style-type: none"> <li>1. Application code not obfuscated and could be decompiled to retrieve initial source code.</li> </ol>	<ol style="list-style-type: none"> <li>1. 8 exported activities, services, and receivers accessible to other services.</li> <li>2. Retrieved source using open-source decompilers</li> </ol>	
MobSF	<ol style="list-style-type: none"> <li>1. Found ELF built without stack protection</li> <li>2. 6 activities are shared with other apps on the device.</li> <li>3. The app uses a weak hash function that should not be used in Secure Crypto.</li> <li>4. App uses insecure Random Number Generator.</li> </ol>	none	<ol style="list-style-type: none"> <li>1. IP address disclosure</li> </ol>	NA

Only the Quixxy tool identified the weak SSL implementation in the Egardia app v2.4.4, which makes the app vulnerable for a MitM attack. With the use of a tooling, the adversary can manipulate the traffic between the app and the cloud service. The figure below shows an example of the a replay attack to disarm the alarm system with PortSwigger Burp. The left pane shows the original request that can be resubmitted with the “Go” button and the right pane shows the response from the cloud service.

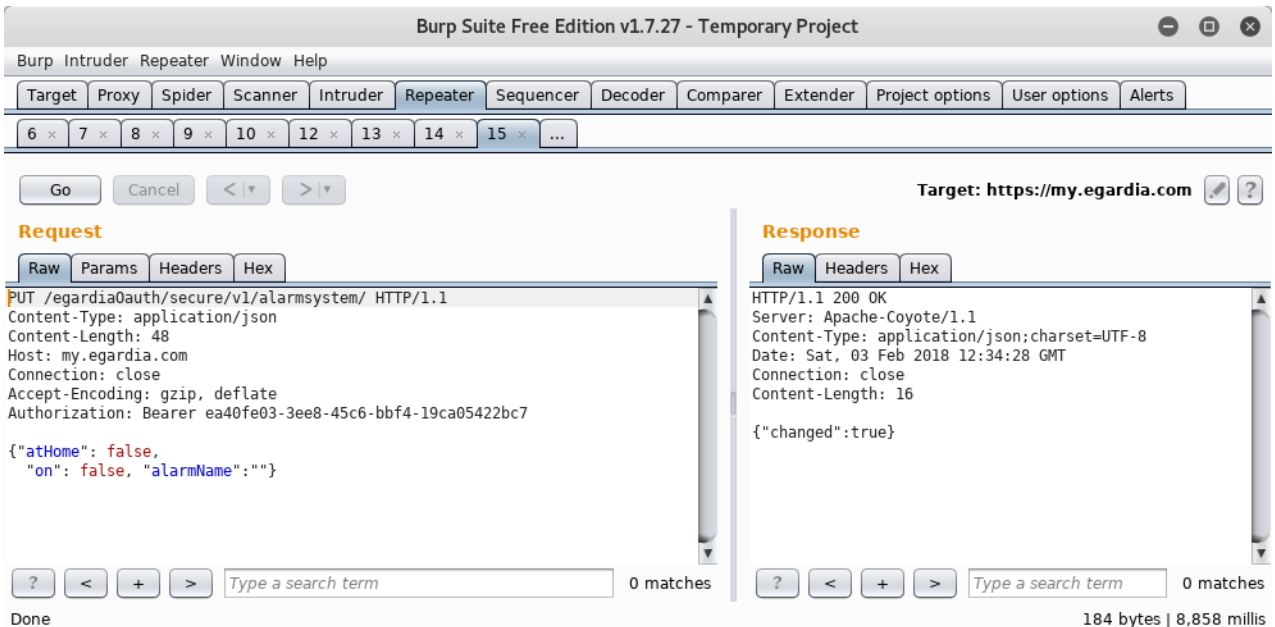


Figure 29: Replay attack by MitM attack using the tool PortSwigger Burp.

Arming and disarming the alarm system through a retransmission of intercepted application data shows that the app has no replay protection. The user’s credentials can also be intercepted with this attack. These harvested credentials can then be used directly on the cloud service. Note, the replay attack will only work for the lifespan of the session token in the authorization header and the app needs trust the certificate authority (CA) that signed the certificate presented by the “man-in-the-middle”. While a

security researcher can do this easily, an adversary has to find other ways to deploy a rogue root certificate on the mobile device. This additional complexity reduces the likelihood of an MitM attack on the traffic between the app and the cloud service.

**CVSS Score and privacy risk**

CVSS Base Score:	9.0			
Impact Subscore:	6.0			
Exploitability Subscore:	2.2			
CVSS Temporal Score:	7.9			
Overall CVSS Score:	7.9			
		<b>Security Risk</b>	<b>Personal Information</b>	<b>Privacy Risk</b>
		High (7.9)	D: PII – Username and password	Medium
<a href="https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:U/RC:R">https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:U/RC:R</a>				

**Conclusion**

The lack of encryption between the gateway and the cloud service makes the alarm system highly vulnerable for a MitM attack. An adversary can retrieve the username and deprecated MD5 password hash from a single captured packet that is transmitted every ten seconds in clear text over the local network and Internet. The MD5 hashing algorithm has known vulnerabilities and passwords hashes can be cracked by a number of publicly available tools. Without cracking the MD5 hash, the adversary can still gain full control over the gateway if the response messages from the cloud services is manipulated. A man in the middle attack can be launched by using malware on any of the systems on the user’s network or by obtaining direct access to the local network. The weaknesses at this layer provide a high security risks, the amount of personal data on the alarm gateway is limited to usage data.

An MitM attack on the app might reveal more personal information, but this attack is less likely to be successful because this communication is adequately encrypted. This a single layer of protection, if this fails for some reason, the personally identifiable data and credentials are disclosed. The overall privacy risk at this layer is assessed as Medium. The leaked credentials, however, lead to a critical privacy risk level on the cloud application and services layer.

**6.4 Layer 4 and 5: The local area network and cloud access layer**

The security of the Local Area Network (LAN) is an important aspect of the security for the Egardia ecosystem. A compromised LAN, wired or wireless, give adversaries logical access to the gateway and the unencrypted traffic between the gateway and the cloud services.

The MitM attacks described in previous paragraphs were performed from the wireless network while the bridge was connected by wire to the switch on the same IP network. By starting an ARP spoofing attack, all traffic from the gateway and app with the cloud services were redirected to the to the workstation on the wireless network. A more detailed description of the attack is provided in Appendix A.

**Risk**

The local network layer and cloud connection layers are the most important layers used by adversaries because they give access to the system. Although not controlled by the user nor the service providers, These layers are still useful in the 6 layer conceptual model to better understand the threats and risks related to the IoT controller layer and cloud application and services layer.

**6.5 Layer 6: Cloud application and services**

A new Egardia alarm system has to be registered by the web application at my.egardia.com. In this registration process, a user account is created and the gateway is linked to this account. The last 3 bytes of the gateway’s mac address are used for identification.

The following information is required by Egardia to create a valid account:

- Salutation
- First name
- Last name
- Address (streetname + number)
- Zip Code
- City
- Country
- Bank Account number (IBAN)
- Email address
- Telephone number
- Mobile number (not required)
- Preferred username
- Password (minimum 6 characters)
- Secret question
- Answer to secret question

Location of the alarm system:

- Address (streetname + number)
- Zip Code
- City
- Country

The information provided to Egardia can be classified as personally identifiable information for an alarm system without surveillance camera. In case one or more surveillance cameras are connected, the personal information is classified as E: Sensitive. According to the manuals, the integration of the camera with the alarm system takes place at the cloud services. Therefore the security and privacy risk for this camera should be assessed separately for the first 5 layers. Security weaknesses in the traditional regular sensors and gateway can have consequences on the privacy risk at the cloud layer.

The Egardia communicates with sh.egardia.com using HTTP and a proprietary messaging system TCP port 52010. The gateway polls the host every 10 seconds as described in 6.3.1 for configuration changes. A short 24 byte message is sent to the cloud service when the status of gateway changes, i.e. when the system is armed or disarmed. The purpose and vulnerabilities of this messaging system were not further investigated. Finally, the gateway periodically determines the public IP address of its Internet connection.

Table 9: Cloud services communicating with the Egardia gateway

#	IP Address	DNS name	Hosting/Service provider	Encryption	Encryption Classification
1	87.250.149.178	sh.egardia.com hosted.by.netground.nl	Netground (KPN cloud services)	HTTP TCP -> port 52010	Na
2	216.146.43.7	checkip.dyndns.com		None	Na

Each http get, post, and put request from the gateway to the cloud service contains the basic authentication header as shown in figure 29. WireShark already decodes the base64 string into a user name and a MD5 hash of the password. The users password can be retrieved by cracking the MD5 hash. The time necessary to crack the password highly depends on the length of the password and the hardware capacity. The hash of password 123456 in the example above only takes a second in a

```

Hypertext Transfer Protocol
  POST /poll/sh HTTP/1.1\r\n
  Authorization: Basic c3B1ZWx0b2Y6ZTEwYWRjMzk0OWJhNTlhYmJ1NTZlMDU3ZjIwZjg4M2U=\r\n
  Credentials: speelt of: e10adc3949ba59abbe56e057f20f883e
  Host: sh.egardia.com\r\n
    
```

Figure 30: Basic authentication header in each http request to the cloud service

dictionary attack. The MD5 hash of an 8 character password containing upper, lower, and special characters can be decrypted in 3

days by leveraging the power of cloud computing[89]. The lack of encryption, the weak password policy of minimal 6 characters, and the lack of salt in the password hash makes the system vulnerable for dictionary attacks on the user’s password.

Similar to the Egardia app, the web application (<https://my.egardia.com>) has no certificate pinning nor replay prevention mechanisms and is therefore vulnerable for the same type of attacks as the app. The

successful MitM attack was used to inspect the actual network traffic on application level. The analysis of this communication showed that Apache/Coyote 1.1 and Liferay Portal Community edition 6.0.4 are used at the cloud application layer. The Liferay portal was released in July 2010 and is outdated and not supported anymore. Furthermore, exploits of these versions are available and include privilege escalations[90][91]. While the use of a community version of software is acceptable for the type of services delivered, the reported version of the software is a significant risk for a large security breach on the cloud application and services layer. The actual vulnerabilities should be assessed by a penetration test on these cloud services, which could not be conducted in this research.

Raw Headers Hex HTML Render	
Name	Value
HTTP/1.1	200 OK
Server	Apache-Coyote/1.1
Set-Cookie	GUEST_LANGUAGE_ID=nl_NL_woonveilig; Expires=Sat, 05-Jan-2019 10:48:37 GMT; Path=/; Secure
Liferay-Portal	Liferay Portal Community Edition 6.0.4 CE (Bunyan / Build 6004 / July 21, 2010)
ETag	f1747658
Content-Type	text/html; charset=UTF-8
Content-Length	22453
Date	Fri, 05 Jan 2018 10:48:37 GMT
Connection	close

Figure 31: Headers in the http communication show that an outdated version of Liferay Portal is used.

The web application in the browser and the apps communicate with several hosts. Especially the communication with connect.triggi.com was a surprise. Egardia’s documentation and information on the public website state that the Egardia alarm system can be integrated with Philips Hue lighting system and several IoT devices. It is not mentioned that this integration is achieved through a third party cloud services called Olisto, formally known as Triggi[92]. There is no possibility for the user to see what data is shared by Egardia with Olisto and the connected service providers. Neither the privacy policies nor the Egardia portal provide insight. Only the app provide the functionality to setup the integration between the alarm and lighting system, but does not mention the use of third party services. Disabling the service does not in provide information on the deletion of personal data.

Table 10: Communication of app and web application with the Egardia cloud services

#	IP Address	DNS name	Hosting/Service provider	Encryption	Encryption Classification
<b>Egardia App</b>					
1	87.250.154.179	my.egardia.com	KPN Internetservices B.V.	TLS v1.2	Qualys A-
2	52.29.232.251	connect.triggi.com	Amazon (Frankfurt Germany)	TLS v1	Qualys A
<b>Browser using the Egardia or Woonveilig web app</b>					
3	87.250.154.37	www.egardia.com	KPN Internetservices B.V	TLS v1.2	Qualys B
4	87.250.154.153	www.woonveilig.nl	KPN Internetservices B.V	TLS v1.2	Qualys B
5	87.250.154.180	alarmsysteem.woonveilig.nl	KPN Internetservices B.V	TLS v1.2	Qualys A-

The server certificates maintained by Egardia have some weaknesses but are assessed as a low security risk.

**CVSS Score and privacy risk**

<b>CVSS Base Score:</b>	9.0	<b>Camera</b>	<b>Security Risk</b>	<b>Personal Information</b>	<b>Privacy Risk</b>
Impact Subscore:	6.0				
Exploitability Subscore:	2.2	No	High (7.9)	D: PII	High
<b>CVSS Temporal Score:</b>	7.9	Yes	High (7.9)	E: Sensitive	Critical
<b>Overall CVSS Score:</b>	7.9				

<https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:U/RC:R>

**Conclusion**

The tests performed at this layer are limited to passive testing and scanning. No penetration tests were performed on the cloud application and services. Indications of vulnerabilities at the cloud service are given by the disclosure of outdated portal services. The main risk at this level for the individual user is that



the credentials captured from one of the MitM attacks on the local network layers can be used to access the cloud services. The weak password policy and password hashing method increase the likelihood of such a successful attack. With the username and cracked password the adversary is able to login in to the cloud services and control the alarm system and obtain personal identifiable information and sensitive information such as life camera footage in case an Egardia surveillance camera purchased. The high security risk with the sensitive personal data leads to a critical privacy risk.

Camera	Security Risk	Personal Information	Privacy Risk
No	High	C: PII	High
Yes	High	D: Sensitive	Critical

## 6.6 Summary of issues in the Egardia ecosystem

The risks identified in this summary apply to a single customer when the risk materializes. All customer data and the related personal information are stored in the cloud services of Egardia. Vulnerabilities in these services could lead to disclosure of potentially all customer data which would be classified as a critical privacy risk. Because no penetration tests were conducted on the cloud services directly the list of vulnerabilities should therefore be regarded as a non-exhaustive list of issues that give a limited insight in the security and privacy risks on the cloud and services layer.

Table 11: Overview of findings with the security and privacy risk assessment for the Egardia Alarm system

Layer	Findings	Security Risk	Personal Info	Privacy risk
1	1. No tampering detection	Medium	A: None	Low
	2. Possible disclosure of personal presence due to continuous operation of sensors when alarm is off.	Low	B: Usage info	Low
2	1. The sensor network can be misused in replay attacks.	Medium	A: None	Low
3	1. Lack of encryption in communication between gateway and cloud services. Through a MitM attack an adversary can obtain full control over the alarm gateway in several ways.	High	D: PII – Username & password	Medium
	2. No certificate pinning nor replay attack prevention on the app allows an adversary to perform a MitM attack on the app.	Medium	D: PII	
	3. Unnecessary http and telnet services running on gateway	Medium	B: Usage info	
6	1. The lack of encryption in the communication and weak authentication based on basic authentication allows an adversary to intercept the basic authentication header and crack the MD5 password hash. These credentials can then be used directly on the cloud services to see the personal and sensitive data.	High	D: PII or Sensitive with use of camera	High Critical with use of camera
	2. No certificate pinning used by the web application at my.egardia.com	Medium	D: PII	
	3. Cloud application is based on outdated community version of Liferay.	High	D: PII	
	4. Uncontrolled sharing and disclosure of personal information caused by using third party services used for integration of services.	Medium	D: PII	

The table above shows that biggest privacy risk is manifested at the cloud application and services layer. This risk is caused by the unencrypted communication between the Egardia gateway and the cloud services. The identified issues are plotted in the privacy risk matrix below. Five high risks have been identified and one of them is assessed as critical when one or more Egardia camera systems are used.

Personal Information	F: Special data				
	E: Sensitive data			(6.1) <sup>10</sup>	
	D: Personal Identification data		(3.2) <sup>11</sup> (6.2) (6.4)	(6.1) <sup>12</sup> (6.3)	
	C: Contact data				
	B: Usage data	(1.2)	(3.3)	(3.1)	
	A: None		(1.1) (2.1)		
		Low	Medium	High	Critical
Information security risk in IoT ecosystem					

Figure 32: Privacy risk matrix for Egardia alarm system

<sup>10</sup> Privacy risk is critical for an Egardia alarm system with surveillance cameras

<sup>11</sup> The overall privacy risk for layer 3 is assessed as medium because of the limited likelihood of a successful MitM attack on app and browser communication with the cloud services.

<sup>12</sup> Privacy risk is high without surveillance camera.

## 6.7 The privacy label for the Egardia Alarm system

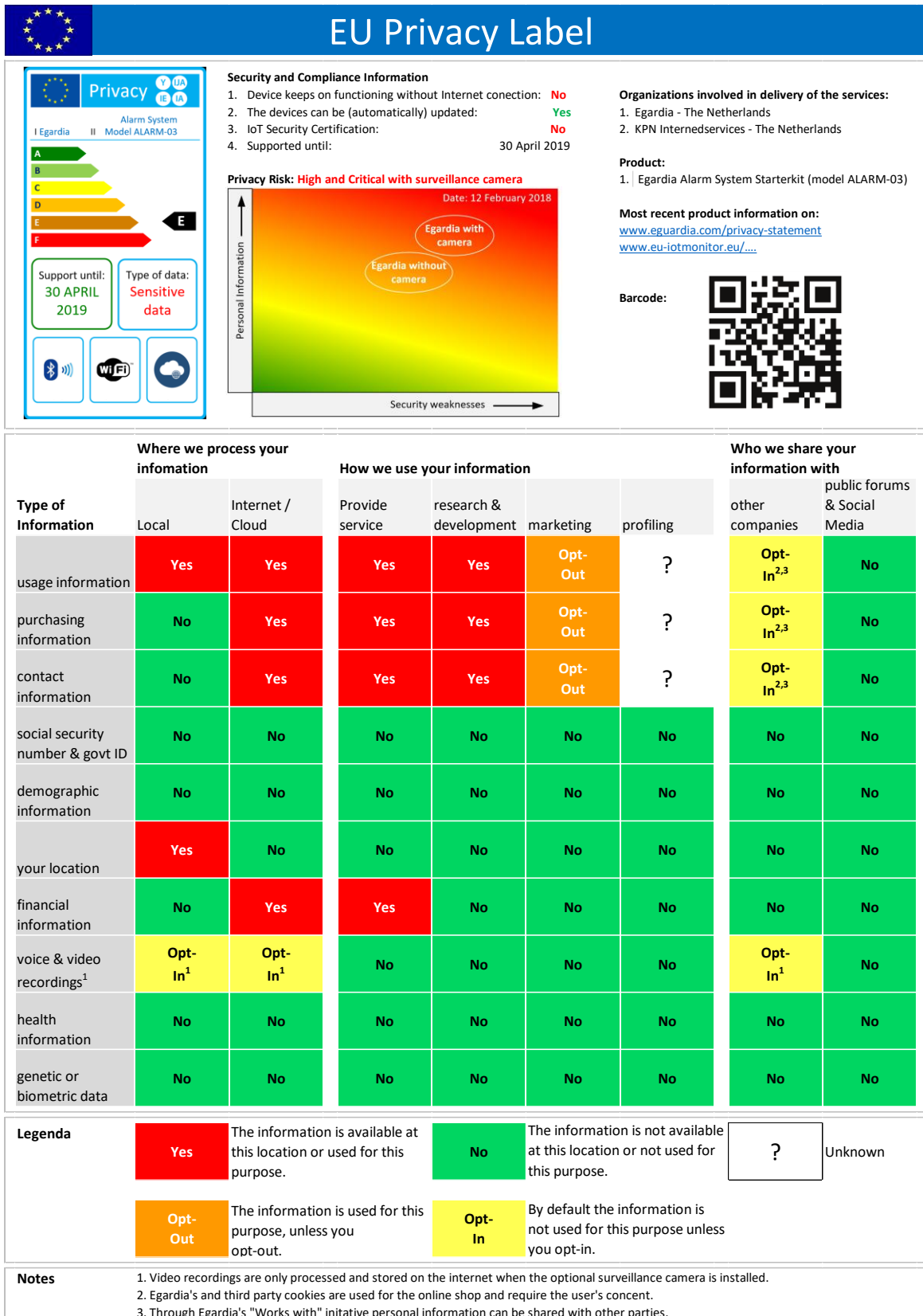


Figure 33: The IoT privacy label for the Egardia alarm system

Note: The “support until” date in the label overview is a fictional date, and intended only as an example.

## 7 Case study 3: The doll “My friend Cayla”.

The doll My friend Cayla, was used in the third case study. Due to the security weaknesses it had a lot of bad publicity and was ultimately banned from the Dutch market in December 2016. The German Federal Network Agency recommended parents to destroy the doll in February 2017 [25][93]. The main problem with Genesis’ Cayla and i-Que robot are considered “toys that spy” and “*the blue-tooth connection allows to listen and talk to the child playing with it*”[94]. Many news articles on the Internet describe what the consequences of the exploited weaknesses are, but they only provide a limited insight what component(s) or security function(s) are actually failing in the ecosystem.

Although the toy is not sold anymore, it has been on the market for two years[95]. Testing the security and privacy of toy’s ecosystem according to the 6 layer model is therefore still useful in order to validate the 6-layer IoT service model and the proposed IoT privacy label. Furthermore the tests in this research (January 2018) show that the cloud services for the interaction conversations with the child have been taken offline. This measure reduces the privacy risk of transmitting the child’s conversations to the cloud service. In this perspective the tests in this research can be seen as a re-evaluation of the ecosystem.

A child can play with the doll in an online mode as well as an offline mode. In online mode a child can have interactive chat sessions with the doll in which the child as well as the doll can ask questions to each other. In offline mode the toy and mobile device can be used to tell stories and playing of games. The stories and games are stored and running on the mobile device as part of the My friend Cayla app.

The whole ecosystem consist of a doll called Cayla, the companion app on an Android or iOS phone or tablet, the cloud services provided by Nuance Communications and Amazon AWS cloud services for hosting Nuance’s services. All questions asked to Cayla are processed by Nuance communications and converted to searches on internet sources such as Google Search, Wikipedia and Weather Underground. The app needs to be installed and active before the toy can be used for playing. In addition, the toy needs to be paired with Bluetooth before the app functions. There is no need to create an account at Genesis, the toy manufacturer or Nuance for the app and toy to operate.

The lab environment in which the My friend Cayla ecosystem was tested is given in the figure below.

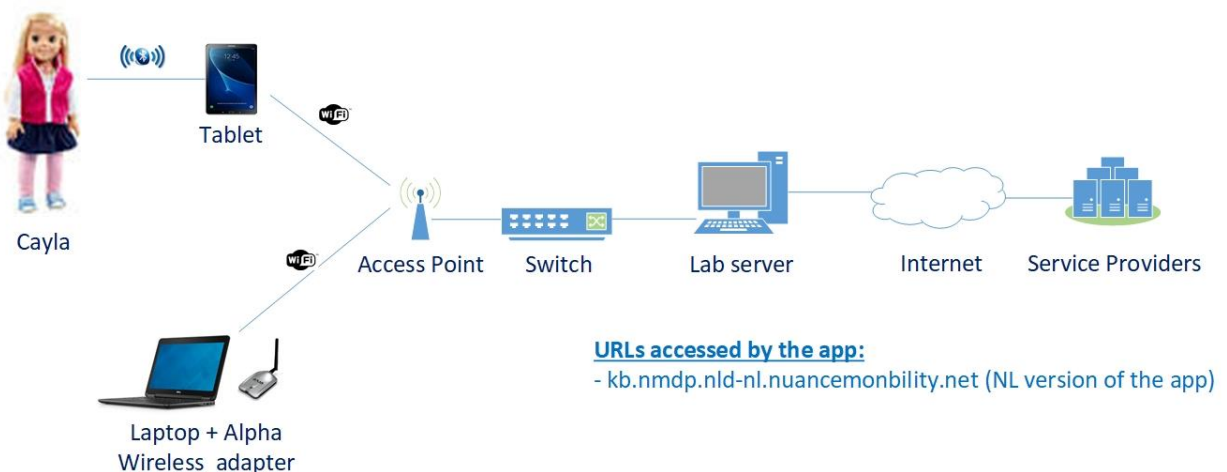


Figure 34: The lab environment to test the My friend Cayla ecosystem.

In ecosystem of My Friend Cayla there is no dedicated device that acts as the gateway between the sensor (the doll) and the cloud service. This functionality is provided by the app installed on a mobile device. A mobile device with a running app is therefore necessary for the functioning of the toy in online and offline mode. The toy ecosystem interacts directly with the child and records and processes the child’s private conversations. The level of personal information is therefore classified as E: Sensitive as defined in table 2.

### 7.1 Layer 1 and 2: The doll Cayla and the Bluetooth connection

The hardware of the doll contains a battery powered circuit board with a Bluetooth receiver/transmitter, a microphone, speaker, and signalling led attached to it. The Bluetooth interface on the device does not require any identification, meaning that any Bluetooth device can connect to the doll that act as a headphone with microphone on an android device as shown in figure 25. A security measure that could have been implemented is a unique PIN code printed on the toy that need to be entered on the Bluetooth device that is pairing to it. Or an button that should be pressed on the toy to be able to pair the toy with an android device. This requires physical access to the toy and will prevent adversaries connecting to the toy from a distance (up to 100 meters in an ideal circumstances and special antennas) [96]. Because the toy has no update facilities, the lack of a pin code for identification in the pairing process could most likely only be resolved by a security recall of sold toys by the manufacturer.

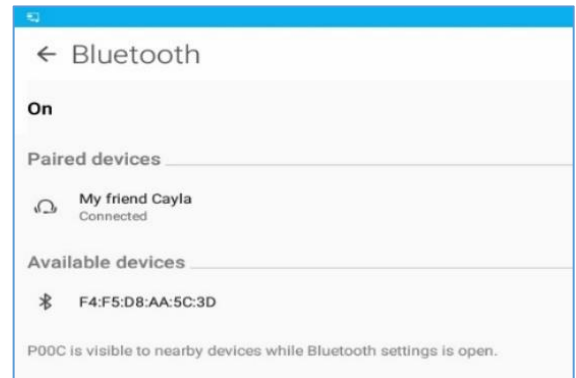


Figure 35: Cayla connects as a Bluetooth headset to the tablet. Although there is a message for a few seconds on the tablet, a pairing code is not needed.

#### CVSS Score and privacy risk

CVSS Base Score:	7.5			
Impact Subscore:	5.3			
Exploitability Subscore:	1.6			
CVSS Temporal Score:	7.1			
Overall CVSS Score:	7.1			
		Security Risk	Personal Information	Privacy Risk
		High (7.1)	E: Sensitive Data	Critical
<a href="https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:L/A:L/E:P/RL:U/RC:C">https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:L/A:L/E:P/RL:U/RC:C</a>				

#### Conclusion

The doll advertises itself as a Bluetooth headset and any Bluetooth device can pair with it to receive the sound recorded by the doll’s microphone or play sound through the dolls speaker like any other Bluetooth headset.

### 7.2 Layer 2: The sensor network

The tablet does not authenticate in any form towards Cayla, which means that an adversary with his own android device can connect to the doll to eavesdrop on all conversations captured by Cayla’s microphone. Freely available Android Apps such as Green Apple Studio’s Audio Recorder, Wonder Grace’s Microphone, and Maxistar’s Mono Bluetooth Router allows the adversary to listen but also speak via the doll’s speaker to the child.

The risks at the sensor network are attributed to the doll and this layer was not further investigated on specific weaknesses in the Bluetooth communication between the toy and the app.

### 7.3 Layer 3: The Cayla app on a mobile device

The app on the mobile device provides several functions and needs to be running for the child to play with the toy. The app does not require an account at the service provider.

In offline mode the doll can tell stories through the speakers while accompanying text and pictures are shown in the app on the mobile device. The text for these stories are stored in clear text in the app and the output of a text-to-speech converter is transmitted over a Bluetooth connection to the toy. An adversary could modify this text allowing the toy to say practically anything.

During the tests performed in March 2017, all questions asked to Cayla in online mode were processed by Nuance communications and converted to searches on internet sources such as Google Search, Wikipedia

and Weather Underground. During the tests in February 2018 the services from Nuance communications have been taken offline. The Dutch and UK versions of the apps have not changed in this period and they still try to connect these services. Since the apps don't get any response, they fall back in a semi-interactive preconfigured conversation in the app. The result is that the child's private conversations are not transmitted to any cloud service. The versions of the app that were used in the tests:

1. My Friend Cayla (Nederlands) v1.0.1 - 15 Sep 2015.
2. My Friend Cayla (EN-UK) v1.0.10 – 14 September 2015

The complaint that has been filed with the Federal Trade Commission by the US Electronic Privacy Information Center (EPIC) states that the Cayla companion application includes a section titled "Child's Information" that prompts children to submit additional information[94]. This functionality was not found in the Dutch version of the App, but is available in the English version of the App (v1.0.10 – 14 Sep 2015). The English version has an additional section Child's information within the Settings area. This section has 20 additional fields that can be set to further 'personalise' the conversation between the child and Cayla. The given data was used in the conversations with Cayla, but it was not clear to what extend this information was shared with Nuance.

Table 12: 20 additional fields with child information in the English (UK) version of the Cayla App

1. My Name is (name)	8. My favourite fairy tale is	14. I like to play
2. My Mum's name is (name)	9. My favourite meal is	15. My favourite book is
3. My Dad's name is (name)	10. My favourite pudding is	16. My favourite film is
4. My favourite cuddly toy is called	11. My favourite ice cream flavour is	17. My favourite song is
5. My favourite TV Program is	12. I go to school at	18. My favourite toy is
6. My favourite sport is	13. My favourite princess is	19. The place I live in is called
7. A musical instrument I like to play is	20. My favourite colour is	

The tests performed in March 2017 showed that the apps were only communicating with the hosts kb.nmdp.nld-nl.nuancemobility.net and kb.nmdp.eng-uk.nuancemobility.net.

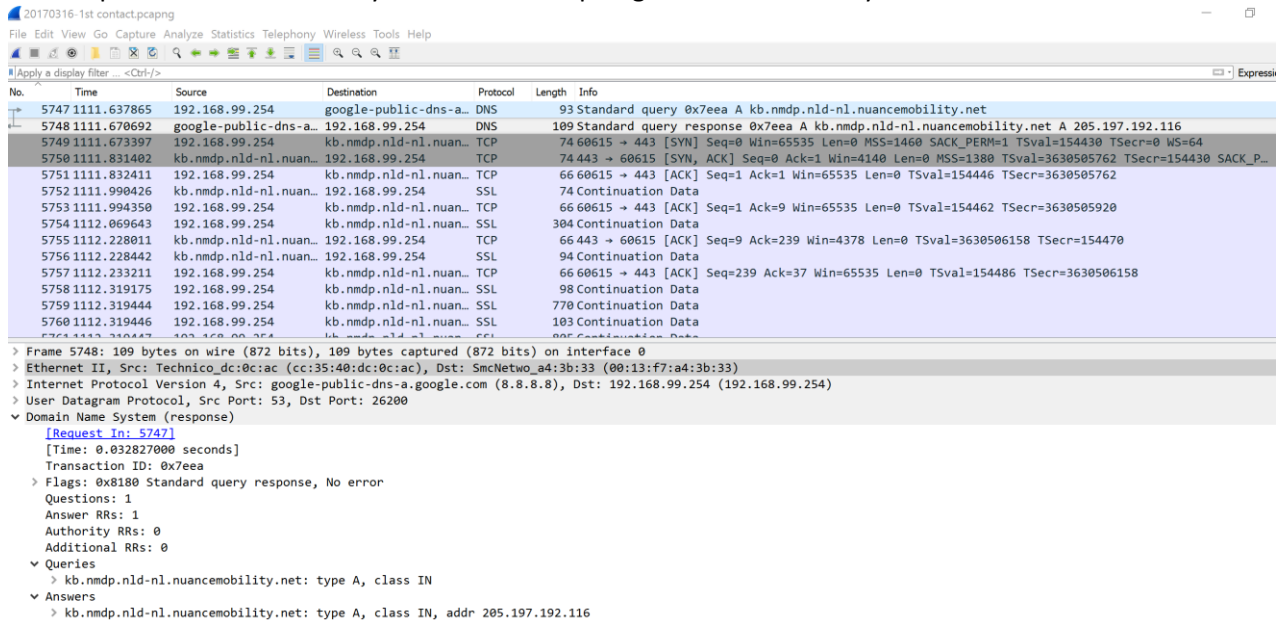


Figure 36: Capture of network traffic between tablet and services provided by Nuance

The captured packets in figure 35 indicate that the data is transmitted over an SSL connection. However further packet inspection showed that there was no real encryption on SSL level. Some information was disclosed, included: type and ID of toy, connection type is Wi-Fi, OS version is 6.0, device is PC001 → Resolves on Google to Asus ZenPad 10 (Z300M/P00C). In addition, the communication from the child to

the cloud service was also transmitted in clear text when the child asks a question to the toy. As shown in the two examples below, the speech is converted in to text on the tablet. Figure 36 below shows the transmitted data over the Internet for the question “Hoeveel is twee plus twee” (How much is two plus two?).

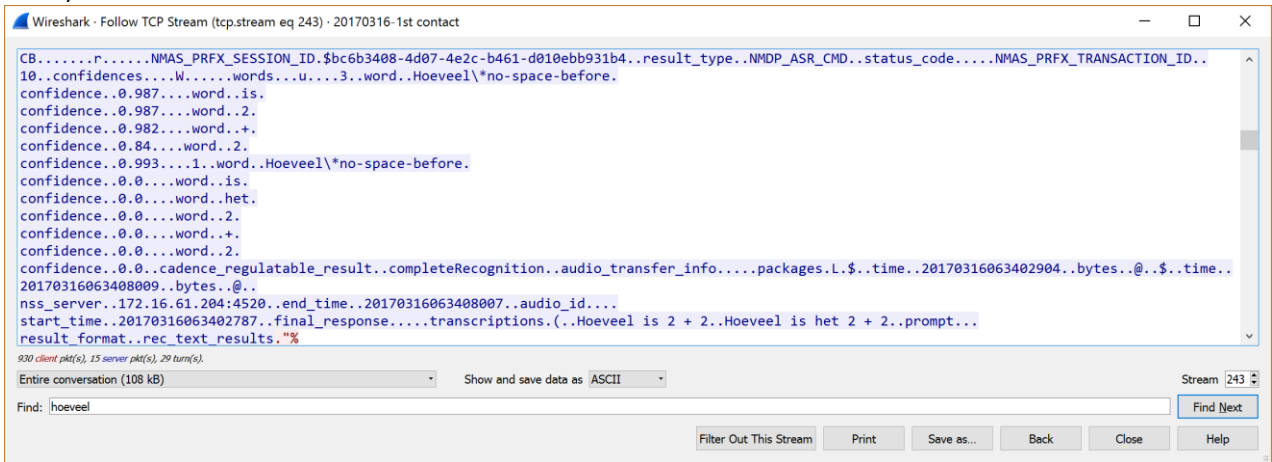


Figure 37: Speech to text conversion of questions

The answer “four” was given by Cayla but not found back in clear text in the captured data. The answer to the question “What is the capital of the Netherlands, Cayla answered “Amsterdam” but this was also not found in clear text in the trace. It could be that the response from the service provider is in raw audio format or that the data is encrypted.

The security of the App was tested by performing automated static code analysis of the app by three different products [28][29][30]. The following table provides the summary of the output of the three different tools.

Table 13: Code review of the My Friend Cayla (Nederlands) v1.0.1 by different tools.

Tool	High risks	Medium Risks	Low risks	Rating
Quixxi	<ol style="list-style-type: none"> <li>1. SSL Implementation check – SSL certificate verification</li> <li>2. File unsafe delete check</li> </ol>	<ol style="list-style-type: none"> <li>1. SQLite Journal Information Disclosure Vulnerability.</li> <li>2. Outputting logs to logcat / logging sensitive information.</li> <li>3. Usage of Adb backup</li> </ol>	<ol style="list-style-type: none"> <li>1. Usage of installer verification code</li> <li>2. Not performing a “Root” or privileged check.</li> </ol>	<p>4.0 / 5</p> <p>Failed 7 out of 34</p>
Ostorlab	<ol style="list-style-type: none"> <li>1. A broadcast receiver is found to be shared with other devices.</li> <li>2. The app uses a weak java hash code</li> </ol>	<ol style="list-style-type: none"> <li>1. Application code not obfuscated and could be decompiled to retrieve initial source code.</li> <li>2. Application does not enforce binary protection.</li> </ol>	<ol style="list-style-type: none"> <li>1. 2 exported activities, services, and receivers accessible to other services.</li> <li>2. Retrieved source using open-source decompilers.</li> <li>3. Backup mode is enabled</li> </ol>	
MobSF	<ol style="list-style-type: none"> <li>1. Insecure implementation of SSL. The application is vulnerable to a MitM attack.</li> <li>2. A broadcast receiver is found to be shared with other devices.</li> <li>3. The app uses a weak hash function that should not be used in Secure Crypto.</li> <li>4. App uses insecure Random Number Generator.</li> </ol>	<ol style="list-style-type: none"> <li>1. Application data can be backed up by Adb.</li> </ol>	<ol style="list-style-type: none"> <li>2. IP address disclosure</li> </ol>	<p>NA</p>

The main weakness in this app was that the app is highly vulnerable for a MitM attack. It is however, fully mitigated by disabling the cloud services. Based on information retrieved from the conversations with the child, the app could learn more about the child over time. These learning capabilities of the app have not been investigated. One of the complaints filed by EPIC was:

*“My Friend Cayla is pre-programmed with dozens of phrases that reference Disneyworld and Disney movies. For example, Cayla tells children that her favorite movie is Disney’s The Little Mermaid and her favorite song is “Let it Go,” from Disney’s Frozen. Cayla also tells children she loves going to Disneyland and wants to go to Epcot in Disneyworld”* [94]. It is not clear if these promotions came from the app itself or from the cloud services.

**CVSS Score and privacy risk**

<b>CVSS Base Score:</b>	8.1	<b>Cloud services</b>	<b>Security Risk</b>	<b>Personal Information</b>	<b>Privacy Risk</b>
Impact Subscore:	5.3	Yes (03-2017)	High (8.1)	E: Sensitive	Critical
Exploitability Subscore:	2.2	No (02-2018)	Medium (6.3)	E: Sensitive	High
<b>CVSS Temporal Score:</b>	7.7				
<b>Overall CVSS Score:</b>	<b>7.7</b>				
<a href="https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:L/A:L/E:P/RL:U/RC:C">https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:L/A:L/E:P/RL:U/RC:C</a> <a href="https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:L/A:L/E:U/RL:U/RC:C">https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:L/A:L/E:U/RL:U/RC:C</a>					

**Conclusion**

The main weakness in this app was that the app is vulnerable for a MitM attack. After the take-down of the cloud services, this risk of a MitM attack is mitigated as no information is communicated to the cloud. The lack of binary protection in the app allow an adversary to run or distribute a modified version of the app. This modified version could contain modified text for the stories or malware to eavesdrop on conversations captured by the toy’s microphone. This risk still exist after shutting down the back-end services.

**7.4 Layer 4 and 5: The local area network and cloud connection layer**

The weak SSL implementation in the app could have been misused when the cloud services were still enabled. In the new situation with the disabled cloud services, a MitM is no longer possible.

**7.5 Layer 6: Cloud services for Cayla**

In the original ecosystem the sensitive play data was sent to Nuance’s cloud services, which give them the possibilities of mass surveillance on children using the toy. Although Nuance did not maintain any account information directly, the combination of sensitive data and the collected app analytic data and metadata such as the device and connection data, IP addresses etc. provide a good base for mass surveillance of children in a particular country.

The complaint filed by EPIC at the FCC include the following high level statements [94]:

1. *Genesis Toys Manufactures, Sells, and Operates Internet-Connected Toys Targeted at Young Children that Collect Personal Information.*
2. *Genesis Toys and Nuance Communications Record and Collect Children’s Voices and Speech Using Voice Recognition Technology on the My Friend Cayla Toy.*
3. *The Terms of Service and Privacy Policy for My Friend Cayla and i-Que Are Confusing and Hard to Access.*
4. *Genesis Toys Fails to Obtain Parental Consent Prior to Collecting, Using, and Disclosing Children’s Voice Recordings via the My Friend Cayla Toy.*
5. *Genesis Retains Children’s Voice Recordings and Other Information Collected via the My Friend Cayla and i-Que Toys for Vague and Potentially Indefinite Periods of Time.*
6. *Genesis Toys Fails to Employ Security Measures to Prevent Unauthorized Access to Personal Information Collected from Children via the My Friend Cayla and i-Que Robot Toys.*



7. *Failure to Provide Adequate Online Notice and Direct Notice to Parents of its Information Practices, and Material Changes Thereto.*
8. *Collection, Use, and Disclosure of Children’s Personal Information Without Obtaining Verifiable Parental Consent*
9. *Failure to Comply with Deletion and Data Retention Requirements.*
10. *Unfair Failure to Employ Reasonable Security Practices to Prevent Unauthorized Bluetooth Connections to the My Friend Cayla and i-Que Dolls.*
11. *Deceptive Failure to Disclose Product Placement in My Friend Cayla and i-Que*
12. *Deceptive Misrepresentation that Genesis Complies with COPPA, but Fails to Obtain Parental Consent or Comply with Other COPPA Requirements.*
13. *Violation of Children’s Online Privacy Protection Act.*
14. *Deceptive Misrepresentation that Nuance is in Compliance with COPPA When it Does Not Obtain Consent From Parents or Provide Other COPPA Procedures.*
15. *Unfair Use of Children’s Voices to Enhance Products and Services Sold to Military, Government, and Law Enforcement Agencies.*

A number of these statements apply to the lack of transparency in the data collection practices and misleading information about compliance to USA regulations. It is likely that the Nuance cloud services were taken offline at some point in time between March 2017 and February 2018 as a result of the official complaint. In the situation as of February 2018 no information is sent to the cloud which reduces the security and privacy risks to none.

**CVSS Score and privacy risk**

<b>CVSS Base Score:</b>	8.1	<table border="1"> <thead> <tr> <th>Cloud services</th> <th>Security Risk</th> <th>Personal Information</th> <th>Privacy Risk</th> </tr> </thead> <tbody> <tr> <td>No (02-2018)</td> <td>None</td> <td>A: None</td> <td>Low</td> </tr> </tbody> </table>	Cloud services	Security Risk	Personal Information	Privacy Risk	No (02-2018)	None	A: None	Low
Cloud services	Security Risk		Personal Information	Privacy Risk						
No (02-2018)	None		A: None	Low						
Impact Subscore:	5.3									
Exploitability Subscore:	2.2									
<b>CVSS Temporal Score:</b>	7.7									
<b>Overall CVSS Score:</b>	<b>7.7</b>									

**7.6 Summary of identified issues**

The risk ratings below are given for the situation in March 2017. At some point in time between March 2017 and February 2018, the Nuance cloud services were taken offline. This mitigated the critical risks related to the potential mass surveillance possibilities. One could argue if the solution is still classifies as an IoT solution after the decommissioning of the cloud services. The risks on the first layer has not been mitigated and still provides a risk to the children playing with the doll.

Table 14: Overview of findings with the security and privacy risk assessment for the Cayla Ecosystem

Layer	Findings	Security Risk	Personal Info	Privacy risk
1	1. No identification of Bluetooth device and toy in the pairing process, allowing any Bluetooth device to pair with the toy and take full control over the toy.	High	E: Sensitive	Critical
2	Not further investigated			
3	1. Several vulnerabilities in the app that could lead to the disclosure of the personally identifiable information of the family and personal preferences and hobbies of the child.	High	High	Critical / high without cloud services
6	1. With the cloud services enabled the weak SSL implementation and the mass surveillance.	None	A: None	Low
	2. Unclear privacy statements	Medium	E: Sensitive	High

The table above shows that the one of the main risks are on the Bluetooth implementation on layers 1 and 2 that allows to take over control of the toy. The second critical issue is the mass surveillance possibilities for Genesis-Toys and Nuance Communications. Weakness in the security controls at these companies could lead to the leakage of these voice recordings.

Personal Information	F: Special data				
	E: Sensitive data		(3.1 <sup>13</sup> ) (6.2)	(1.1) (3.1) <sup>14</sup>	
	D: Personal Identification data				
	C: Contact data				
	B: Usage data				
	A: None	(6.1)			
		Low	Medium	High	Critical
Information security risk in IoT ecosystem					

Figure 38: Privacy risk matrix for the Cayla eco system.

<sup>13</sup> The privacy risk is high in the situation with disabled cloud services.

<sup>14</sup> The situation in March 2017 had the cloud services enabled which leads to a critical privacy risk.

### 7.7 The IoT privacy label for Genesis' My Friend Cayla



Figure 39: The IoT privacy label for toy My Friend Cayla

Note: The “support until” date in the label overview is a fictional date, and intended only as an example.

## 8 Conclusion, recommendations and reflection

The case studies showed that the developed methodologies can be used to fill-out the privacy label to a large extent. The same methodologies and privacy label design can be used for very different IoT products. Collaboration with manufacturer and service provider(s) are necessary to fill out the complete privacy label. Information such as with whom the information is shared and for what purpose needs to be provided by the manufacturer and the service providers. Also the penetration testing on cloud applications and services should have been performed with approval of the service owner to provide a reasonable assurance to customers about the privacy risks. The populated privacy labels for the IoT products used in the case studies should not be considered as complete because the performed tests at the cloud application layer were too limited to provide a reasonable assurance about the privacy risk.

Unlike energy labels, there are many more parameters in information security and privacy than just electricity and fuel consumption. Therefore the privacy label needs to balance between the level of detail and the understandability of the information by consumers. Furthermore, the security measures deteriorate over time, meaning that the privacy risks increase over time. This would plea for a more dynamic approach of the privacy label, so that the user can assess if he or she still wants to use the product, or replace it with a newer and more secure system. Such a dynamic centrally registered privacy classification requires that products are assessed periodically. This could be part of the monitoring function as suggested by the Dutch and European agencies. A European or worldwide implementation of such a system will require several years due to the large number of stakeholders and the current state of the recommendations given by the Dutch Cyber Security Council and ENISA.

Performing security testing on an IoT ecosystem is actually a combination of penetration testing on various components and technologies. Each component has its own set of tools that need to be tailored for the task at hand. Many opensource tools are available which reduces the cost to setup a lab. However tailoring the tools and learn how they work is a time consuming task. Another downside of using opensource tools is the limited support and the different outcomes of scans by similar code and vulnerability scanners.

### 8.1 Recommendations

Several weaknesses were encountered in the case studies. The following technical measures are recommended for home networks to avoid a security breach:

1. Enforce unique strong passwords for each system or service that requires credentials.
2. Implement Network Access Control so that only authorized devices can connect to the (wireless) network.
3. Create different networks in the house separated by firewall rules or Access Control lists.
4. When a device is no longer used, reset the devices to factory default so that all personal data is removed from the device or destroy the device physically when a factory reset cannot be done (anymore).

The problem with these recommendations is that consumers generally do not have the skills to implement these measures. New standards and technology is necessary in the future that would make securing networks much simpler. In the meanwhile, manufacturers and service providers should take the appropriate security measures so that the risk of product misuse or leakage of personal data is kept to a minimum. Although very generic, manufactures and service providers should deliver products that:

1. Treat local networks as insecure networks to prevent security breaches from a poorly secured local network.
2. Enforce users to use strong passwords, in case the IoT system is some kind of security related system such as an alarm system or smart lock provide the opportunity for strong authentication.

3. Have appropriate authentication and authorization at each component in the chain of the IoT solution.
4. Ensure adequate encryption of data in transport between all components that are part of the solution.
5. Implement specific measures to avoid replay attacks in any of the communication channels because encryption does not necessarily protect against replay attacks [97]. Replay attacks can be avoided or at least made much more difficult by an adversary when a cryptographic nonce is used in the communication paths.
6. Implement a reset function that will reset the cryptographic keys to lockout intruders.
7. Provide transparency to the customer in what data is actually shared with business partners and IoT integration parties such as Triggs [98].

## 8.2 Further research

Further research is recommended in a number of areas, including:

1. The effectiveness of the privacy label – Is the designed privacy label effective enough and how can it become more dynamic to cope with the fluctuation in security and privacy risk? Security and privacy risks increase when software becomes outdated but decrease when the software is maintained and patched.
2. The governance model for the implementation of the privacy label through. Especially when a central monitoring function is deployed within the EU.
3. The economical aspects of the introduction of a privacy label.
4. What norms and standards should be used by the security testers. In this research the scope of the tests cover the entire IoT ecosystem. The depth of the tests was not covered in this research.

## Bibliography

- [1] 'Internet of Things Global Standards Initiative', *ITU*. [Online]. Available: <http://www.itu.int:80/en/ITU-T/gsi/iot/Pages/default.aspx>. [Accessed: 08-Nov-2017].
- [2] 'Internet of things', *Wikipedia*. 08-Nov-2017.
- [3] 'Maak kennis met de Nest Learning Thermostat', *Nest*. [Online]. Available: <https://www.nest.com/nl/thermostats/nest-learning-thermostat/overview/>. [Accessed: 08-Nov-2017].
- [4] 'Hoe werkt de Ecotemperatuur op de Nest Thermostat?', *Nest*. [Online]. Available: <https://www.nest.com/nl/support/article/>. [Accessed: 08-Nov-2017].
- [5] Philips Lighting, 'Friends of Hue - Meethue', *Philips Lighting*. [Online]. Available: <http://www2.meethue.com/en-us/friends-of-hue>. [Accessed: 16-Dec-2017].
- [6] Enguardia, 'Works with Egardia | Egardia'. [Online]. Available: <https://www.egardia.com/en/works-with>. [Accessed: 16-Dec-2017].
- [7] 'Gartner Says 6.4 Billion Connected'. [Online]. Available: <https://www.gartner.com/newsroom/id/3165317>. [Accessed: 08-Nov-2017].
- [8] A. Nordrum, 'Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated', *IEEE Spectrum: Technology, Engineering, and Science News*, 18-Aug-2016. [Online]. Available: <https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated>. [Accessed: 08-Nov-2017].
- [9] K. L. Lueth, 'IoT market segments – Biggest opportunities in industrial manufacturing - IoT Analytics'. [Online]. Available: <https://iot-analytics.com/iot-market-segments-analysis/>. [Accessed: 09-Nov-2017].
- [10] 'Consumer Internet of Things (CIoT) - what is it and how does it evolve?', *i-SCOOP*. [Online]. Available: <https://www.i-scoop.eu/internet-of-things-guide/what-is-consumer-internet-of-things-ciot/>. [Accessed: 22-Nov-2017].
- [11] K. L. Lueth, 'IoT Market - Forecasts at a glance - IoT Analytics'. [Online]. Available: <https://iot-analytics.com/iot-market-forecasts-overview/>. [Accessed: 22-Nov-2017].
- [12] H. Sim, 'Voice Assistants: This Is What The Future Of Technology Looks Like', *Forbes*. [Online]. Available: <https://www.forbes.com/sites/herbertsim/2017/11/01/voice-assistants-this-is-what-the-future-of-technology-looks-like/>. [Accessed: 23-Nov-2017].
- [13] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, 'The Internet of Things for Health Care: A Comprehensive Survey', *IEEE Access*, vol. 3, pp. 678–708, 2015.
- [14] M. van J. en Veiligheid, 'Towards a safe, connected, digital society - Recommendation on the cybersecurity of the Internet of Things (IoT)', 26-Apr-2018. [Online]. Available: [https://www.cybersecurityraad.nl/030\\_Publicaties/](https://www.cybersecurityraad.nl/030_Publicaties/). [Accessed: 13-May-2018].
- [15] M. van E. Z. en Klimaat, 'Onveilige apparatuur risico voor samenleving - Staat van de Ether'. [Online]. Available: <https://magazines.agentschaptelecom.nl/staatvandeether/2018/01/onveilige-apparatuur-risico-voor-samenleving>. [Accessed: 05-Jun-2018].
- [16] 'Proposal European Cybersecurity Act'. [Online]. Available: [https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477\\_en](https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en). [Accessed: 05-Jun-2018].
- [17] 'Baseline Security Recommendations for IoT — ENISA'. [Online]. Available: <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>. [Accessed: 05-Jun-2018].
- [18] 'IoT Framework Assessment - OWASP'. [Online]. Available: [https://www.owasp.org/index.php/IoT\\_Framework\\_Assessment](https://www.owasp.org/index.php/IoT_Framework_Assessment). [Accessed: 08-Nov-2017].
- [19] 'IoT Testing Guides - OWASP'. [Online]. Available: [https://www.owasp.org/index.php/IoT\\_Testing\\_Guides](https://www.owasp.org/index.php/IoT_Testing_Guides). [Accessed: 08-Nov-2017].
- [20] A. R. Hevner, S. T. March, J. Park, and S. Ram, 'Design science in information systems research', *MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004.
- [21] 'CVSS v3.0 Specification Document', *FIRST — Forum of Incident Response and Security Teams*. [Online]. Available: <https://www.first.org/cvss/specification-document>. [Accessed: 17-Mar-2018].

- [22] Philips Lighting, 'Philips Lighting Annual Report 2016'. 16-Feb-2017.
- [23] 'WoonVeilig'. [Online]. Available: <https://www.woonveilig.nl/reviews>. [Accessed: 15-Jan-2018].
- [24] 'My Friend Cayla', *My Friend Cayla*. [Online]. Available: <https://www.myfriendcayla.com>. [Accessed: 16-Dec-2017].
- [25] 'Germany bans creepy doll over privacy concerns', *Engadget*. [Online]. Available: <https://www.engadget.com/2017/02/17/germany-bans-my-friend-cayla-doll/>. [Accessed: 19-Feb-2017].
- [26] 'GNU Radio', *Wikipedia*. 09-Aug-2017.
- [27] M. Ossmann, 'Great Scott Gadgets - HackRF One', *HackRF One*. [Online]. Available: <https://greatscottgadgets.com/hackrf/>. [Accessed: 16-Dec-2017].
- [28] *Mobile-Security-Framework-MobSF: Mobile Security Framework is an intelligent, all-in-one open source mobile application (Android/iOS/Windows) automated pen-testing framework capable of performing ..* Mobile Security Framework, 2018.
- [29] 'Integrated App Analytics, Mobile App Security and Control', *Quixxi*. [Online]. Available: <https://quixxi.com/>. [Accessed: 10-Jan-2018].
- [30] 'Ostorlab Cloud Based Mobile Application Security, Vulnerability Scanner for Android and iOS'. [Online]. Available: <https://www.ostorlab.co>. [Accessed: 10-Jan-2018].
- [31] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, 'A roadmap for security challenges in the Internet of Things', *Digit. Commun. Netw.*, Apr. 2017.
- [32] 'ISO/IEC 29100:2011 - Information technology -- Security techniques -- Privacy framework'. [Online]. Available: <https://www.iso.org/standard/45123.html>. [Accessed: 23-Mar-2018].
- [33] M. G. Michael, *Ubervveillance and the Social Implications of Microchip Implants: Emerging Technologies: Emerging Technologies*. IGI Global, 2013.
- [34] The European Parliament, 'REGULATION (EU) 2016/679', 04-May-2016. [Online]. Available: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. [Accessed: 19-Mar-2017].
- [35] 'ISO/IEC 27005:2011(en), Information technology — Security techniques — Information security risk management'. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en>. [Accessed: 30-Mar-2017].
- [36] Nederlands Normalisatie-instituut, 'Nen-iso/iec 31010', 2014.
- [37] 'Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings', *Motherboard*. [Online]. Available: [https://motherboard.vice.com/en\\_us/article/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings](https://motherboard.vice.com/en_us/article/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings). [Accessed: 19-Mar-2017].
- [38] L. Franceschi-Bicchierai, 'One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids', *Motherboard*, 27-Nov-2015. [Online]. Available: [https://motherboard.vice.com/en\\_us/article/yp3z5v/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids](https://motherboard.vice.com/en_us/article/yp3z5v/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids). [Accessed: 04-Apr-2018].
- [39] Philips Lighting, 'Privacy Notice - Meethue', *Philips Lighting*. [Online]. Available: <http://www2.meethue.com/en-us/support/privacy-notice>. [Accessed: 21-Jan-2018].
- [40] 'Privacy statement | Egardia'. [Online]. Available: <https://www.egardia.com/en/privacy-statement>. [Accessed: 01-Apr-2018].
- [41] 'Anatomy of an IoT malware attack (and what to do to prevent one)', 31-Oct-2017. [Online]. Available: <http://www.ibm.com/developerworks/library/iot-anatomy-iot-malware-attack/index.html>. [Accessed: 01-Apr-2018].
- [42] T. Moore, 'The economics of cybersecurity: Principles and policy options', *Int. J. Crit. Infrastruct. Prot.*, vol. 3, no. 3–4, pp. 103–117, 2010.
- [43] M. Stevens, E. Bursztein, and P. Karpman, 'Announcing the first SHA1 collision', *Google Online Security Blog*. .
- [44] R. Koenes, 'Eigenaar sauna: beelden Oranje-handbalsters gestolen bij hack', *AD.nl*, 07-Mar-2018. [Online]. Available: <https://www.ad.nl/binnenland/eigenaar-sauna-beelden-oranje-handbalsters-gestolen-bij-hack~aa6bbae3/>. [Accessed: 01-Apr-2018].

- [45] M. Nieuwenhuis, 'Naaktbeelden van zeker honderd saunagasten Nederasselt staan nog steeds online', *AD.nl*, 08-Mar-2018. [Online]. Available: <https://www.ad.nl/binnenland/naaktbeelden-van-zeker-honderd-saunagasten-nederasselt-staan-nog-steeds-online~abb08884/>. [Accessed: 01-Apr-2018].
- [46] S. L. Heinzle and R. Wüstenhagen, 'Dynamic Adjustment of Eco-labeling Schemes and Consumer Choice—the Revision of the EU Energy Label as a Missed Opportunity?', *Bus. Strategy Environ.*, vol. 21, no. 1, pp. 60–70, 2012.
- [47] 'P3P: The Platform for Privacy Preferences'. [Online]. Available: <https://www.w3.org/P3P/>. [Accessed: 29-Apr-2018].
- [48] R. W. Reeder, P. G. Kelley, A. M. McDonald, and L. F. Cranor, 'A user study of the expandable grid applied to P3P privacy policy visualization', in *Proceedings of the 7th ACM workshop on Privacy in the electronic society*, 2008, pp. 45–54.
- [49] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, 'A "Nutrition Label" for Privacy', in *Proceedings of the 5th Symposium on Usable Privacy and Security*, New York, NY, USA, 2009, pp. 4:1–4:12.
- [50] M. van V. en Justitie, 'IoT-toepassingen vormen bedreiging voor veiligheid en privacy', 18-Jan-2018. [Online]. Available: [https://www.cybersecurityraad.nl/010\\_Actueel/iot-toepassingen-vormen-bedreiging-voor-veiligheid-en-privacy.aspx](https://www.cybersecurityraad.nl/010_Actueel/iot-toepassingen-vormen-bedreiging-voor-veiligheid-en-privacy.aspx). [Accessed: 23-Jan-2018].
- [51] '2net™ platform', *Qualcomm*, 12-Mar-2014. [Online]. Available: <https://www.qualcomm.com/products/2net>. [Accessed: 13-May-2018].
- [52] 'The Platform for Privacy Preferences 1.1 (P3P1.1) Specification'. [Online]. Available: [https://www.w3.org/TR/P3P11/#base\\_data\\_structure](https://www.w3.org/TR/P3P11/#base_data_structure). [Accessed: 05-May-2018].
- [53] 'Aantal zorgsites stopt met tracking-pixel van Facebook'. [Online]. Available: <https://nos.nl/artikel/2226957-aantal-zorgsites-stopt-met-tracking-pixel-van-facebook.html>. [Accessed: 13-May-2018].
- [54] S. Li, L. D. Xu, and S. Zhao, 'The internet of things: a survey', *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, Apr. 2015.
- [55] P. Scully and K. L. Lueth, 'Guide to IoT Solution Development'. [Online]. Available: <https://iot-analytics.com/guide-to-iot-solution-development/>. [Accessed: 16-Dec-2017].
- [56] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, 'Edge computing: Vision and challenges', *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, 2016.
- [57] IBM X-Force Research, 'The inside story on botnets', 27-Feb-2017. [Online]. Available: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEL03086USEN&attachment=SEL03086USEN.PDF>. [Accessed: 16-Jan-2018].
- [58] IBM X-Force Research, 'The weaponization of IoT devices', 05-Apr-2017. [Online]. Available: <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03128USEN>. [Accessed: 16-Jan-2018].
- [59] M. Bing, 'The Lizard Brain of LizardStresser', *Arbor Networks Threat Intelligence*, 29-Jun-2016. [Online]. Available: <https://www.arbornetworks.com/blog/asert/lizard-brain-lizardstresser/>. [Accessed: 16-Jan-2018].
- [60] R. Roman, J. Zhou, and J. Lopez, 'On the features and challenges of security and privacy in distributed internet of things', *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013.
- [61] R. Roman, J. Lopez, and M. Mambo, 'Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges', *Future Gener. Comput. Syst.*, 2016.
- [62] 'MAC flooding', *Wikipedia*. 10-Jan-2018.
- [63] D. R. Raymond and S. F. Midkiff, 'Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses', *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 74–81, Jan. 2008.
- [64] A. Sikora, P. Lehmann, N. Anantalapochai, M. Dold, D. Rahusen, and A. Rohleder, 'Recent Advances in EN13757 Based Smart Grid Communication', *J. Commun.*, vol. 9, no. 9, 2014.
- [65] P. P. Ray, 'A survey on Internet of Things architectures', *J. King Saud Univ. - Comput. Inf. Sci.*, Oct. 2016.



- [66] S. H. Eikenberg Ronald, 'Home security systems hacked with 1234 password', *c't*. [Online]. Available: <https://www.heise.de/ct/artikel/Home-security-systems-hacked-with-1234-password-3248831.html>. [Accessed: 16-Jan-2018].
- [67] OWASP, 'Mobile Top 10 2016-Top 10 - OWASP'. [Online]. Available: [https://www.owasp.org/index.php/Mobile\\_Top\\_10\\_2016-Top\\_10](https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10). [Accessed: 16-Jan-2018].
- [68] 'OWASP Mobile Security Testing Guide - OWASP'. [Online]. Available: [https://www.owasp.org/index.php/OWASP\\_Mobile\\_Security\\_Testing\\_Guide#tab=Main](https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide#tab=Main). [Accessed: 16-Jan-2018].
- [69] 'title:"hue personal wireless lighting" - Shodan Search'. [Online]. Available: [https://www.shodan.io/search?query=title:"hue+personal+wireless+lighting"](https://www.shodan.io/search?query=title:). [Accessed: 17-Dec-2017].
- [70] OWASP, 'Top 10-2017 Top 10 - OWASP'. [Online]. Available: [https://www.owasp.org/index.php/Top\\_10-2017\\_Top\\_10](https://www.owasp.org/index.php/Top_10-2017_Top_10). [Accessed: 17-Jan-2018].
- [71] P. P. Ray, 'A survey of IoT cloud platforms', *Future Comput. Inform. J.*, vol. 1, no. 1, pp. 35–46, Dec. 2016.
- [72] 'OAuth 2.0 — OAuth'. [Online]. Available: <https://oauth.net/2/>. [Accessed: 07-Jan-2018].
- [73] ISO, 'Certification'. [Online]. Available: <https://www.iso.org/certification.html>. [Accessed: 06-Jun-2018].
- [74] AICPA, 'SOC for Service Organizations: Information for Service Organizations', *AICPA*. [Online]. Available: <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smmanagement.html>. [Accessed: 16-Jan-2018].
- [75] AICPA, 'Trust Services and Information Integrity', *AICPA*. [Online]. Available: <https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/trustdataintegritytaskforce.html>. [Accessed: 16-Jan-2018].
- [76] 'How hue works | Philips Hue API'. [Online]. Available: <https://developers.meethue.com/documentation/how-hue-works>. [Accessed: 17-Dec-2017].
- [77] R. L. Security, *killerbee: IEEE 802.15.4/ZigBee Security Research Toolkit*. 2018.
- [78] T. Zillner and S. Strobl, 'ZigBee exploited: The good the bad and the ugly', *Magdebg. J. Zur Sicherheitsforschung*, vol. 12, pp. 699–704, Sep. 2016.
- [79] P. Morgner, S. Mattejat, and Z. Benenson, 'All your bulbs are belong to us: Investigating the current state of security in connected lighting systems', *ArXiv Prepr. ArXiv160803732*, 2016.
- [80] ZigBee Alliance, 'Zigbee Light Link Standard'. ZigBee Alliance, 05-Apr-2012.
- [81] P. Morgner, S. Mattejat, Z. Benenson, C. Müller, and F. Armknecht, 'Insecure to the touch: attacking ZigBee 3.0 via touchlink commissioning', in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2017, pp. 230–240.
- [82] 'Philips Hue - Bridge Firmware Release notes', *Philips Lighting*. [Online]. Available: <http://www2.meethue.com/en-us/support/release-notes/bridge>. [Accessed: 14-Jan-2018].
- [83] IoTsec, 'Z3sec: Penetration testing framework for ZigBee security research', 28-May-2018. [Online]. Available: <https://github.com/IoTsec/Z3sec>. [Accessed: 11-Jan-2018].
- [84] C. O'Flynn, 'Getting Root on Philips Hue Bridge 2.0'. [Online]. Available: <http://colinoflynn.com/2016/07/getting-root-on-philips-hue-bridge-2-0/>. [Accessed: 07-Jan-2018].
- [85] Qualys Inc., 'Qualys Vulnerability Management'. [Online]. Available: <https://www.qualys.com/suite/vulnerability-management/>. [Accessed: 11-Jun-2017].
- [86] S. Hansen and R. Eikenberg, 'Sicherheitslecks in vernetzten Alarmsystemen', *c't Smart Home (2016): Der Praxis-Guide für intelligentes Wohnen*, pp. 32–35.
- [87] N. Abel, D. Dilger, T. Herres, and S. Kettler, 'Multiple vulnerabilities in Lupusec XT1 Alarm System', *Foxmole*, 28-Oct-2016. [Online]. Available: [https://www.foxmole.com/foxmole\\_en/advisories/foxmole-2016-07-20.txt](https://www.foxmole.com/foxmole_en/advisories/foxmole-2016-07-20.txt). [Accessed: 16-Jan-2018].
- [88] Federal Communications Commission IDentification, 'HPGW Gateway User Manual Users Manual Climax Technology Co Ltd', *FCCID.io*. [Online]. Available: <https://fccid.io/GX9HPGW/User-Manual/Users-Manual-2771759>. [Accessed: 02-Feb-2018].

- [89] P. Kamal, 'A Study on the Security of Password Hashing Based on GPU Based, Password Cracking using High-Performance Cloud Computing', *Culminating Proj. Inf. Assur.* 25, 2017.
- [90] J. Kuperus, 'Liferay Portal 6.0.x < 6.1 - Privilege Escalation', *Exploit Database*. [Online]. Available: <https://www.exploit-db.com/exploits/18881/>. [Accessed: 04-Feb-2018].
- [91] 'Liferay Portal 6.2 - Liferay Developer Network'. [Online]. Available: <https://dev.liferay.com/web/community-security-team/known-vulnerabilities/liferay-portal-62>. [Accessed: 04-Feb-2018].
- [92] 'Met Olisto haal je het meeste uit je slimme apparaten', *Olisto*, 04-Oct-2017. .
- [93] 'German parents told to destroy Cayla dolls over hacking fears', *BBC News*, 17-Feb-2017. [Online]. Available: <http://www.bbc.com/news/world-europe-39002142>. [Accessed: 19-Feb-2017].
- [94] The Electronic Privacy Information Center (EPIC), 'In re: Genesis Toys and Nuance Communication. Complaint and Request for Investigation, Injunction, and Other Relief.' Federal Trade Commission, 12-Jun-2016.
- [95] 'Speelgoedpop "My Friend Cayla" blijkt kinderen af te luisteren'. [Online]. Available: <http://nos.nl/artikel/2146787-speelgoedpop-my-friend-cayla-blijkt-kinderen-af-te-luisteren.html>. [Accessed: 01-Apr-2017].
- [96] J. G. Sponås, 'Things you should know about Bluetooth range'. [Online]. Available: <http://blog.nordicsemi.com/getconnected/things-you-should-know-about-bluetooth-range>. [Accessed: 02-Apr-2017].
- [97] P. Syverson, 'A taxonomy of replay attacks [cryptographic protocols]', in *Computer Security Foundations Workshop VII, 1994. CSFW 7. Proceedings, 1994*, pp. 187–191.
- [98] 'Triggi makes smart thing smarter, according to your rules.', *Triggi*. [Online]. Available: <https://triggi.com/?lang=en>. [Accessed: 07-Jan-2018].
- [99] G. Hernandez, O. Arias, D. Buentello, and Y. Jin, 'Smart nest thermostat: A smart spy in your home', *Black Hat USA*, 2014.

## Appendix A: MitM attacks on Philips Hue and Egardia alarm systems

For the three IoT devices that were investigated could be a target for adversaries. Depending on the goals and motive of the adversary, the individual device could be targeted or all that particular devices could be targeted for the deployment of malware. Deploying botnets on IoT devices would remain undetected because there are no virus or malware scanners active on these systems, neither is their behaviour monitored in a consumer environment. Although IoT devices have limited processing power, they have connection to the Internet and can be used on a massive scale for DDOS attacks. In order to deploy the botnets on such a massive scale, the process has to be automated to be effective. The most obvious processes to be attacked are the manufacturing and distribution processes and the firmware update distribution process. The consumer is depending on the security measures of the service providers for this type of attacks.

An attack on a single system could take place in several ways, there are many attack surfaces. If the adversary is aware of the target's address and the WiFi connection is in the same network as the target device, then the following scenario could be possible due to the lack of or weak encryption on the local LAN. By attacking the WiFi network, the adversary does not have to enter the premises of the target. Some of the successful attacks on the Philips Hue bridge and NEST thermostat described on the Internet require physical access to the device and would therefore be more risky for the adversary [84][99]. An attack that can be launched in the proximity of the target premises would take the following steps

1. Obtain access to the target WiFi network using common tools such as airmon-ng, airodump-ng, aireplay-ng packets of the target WiFi network. Subsequently a brute force attack with aircrack-ng can be launched on the captured packets in order to crack the WiFi networks password. The procedures for breaking into a WiFi network is well described on the Internet. A search for "hack wifi password" on Google gives almost 1,9 million hits.
2. Find the target IoT devices on the local network by running a quick scan on the network with tools like nmap or zenmap to identify the connected devices, their IP addresses and especially the MAC addresses in this stage. The MAC addresses indicate the type of device and in this experiment, the Philips Hue bridges and Egardia gateways can be recognized by their MAC address as shown in the figure below.

```
Nmap scan report for 192.168. [redacted]
Host is up (0.037s latency).
Not shown: 98 closed ports
PORT      STATE SERVICE
80/tcp    open  http
8080/tcp  open  http-proxy
MAC Address: 00:17:88: [redacted] (Philips Lighting BV)
```

```
Nmap scan report for 192.168. [redacted]
Host is up (0.0097s latency).
Not shown: 99 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 50:50:2A: [redacted] (Egardia)
```

Figure 40: Output of simple scan to identify target devices

3. Now a Man-in-the-Middle (MitM) attack can be launched by redirecting network traffic from the IoT device to the adversary's system by using arp poisoning. There are ways to protect against arp spoofing but these measures are generally not implemented in home networks. By using an arp poisoning tool on Linux such as:

```
arpspoof -i <interface name> -t <target IP address> -r <default gateway>
```

This command tells the target machine that the default gateway is located at the MAC address of

- the adversary's system. Hence the target system now sends the network traffic through the adversary's PC who can eavesdrop on all unencrypted traffic sent to and from the target device.
4. Intercepted cleartext passwords can be used directly on the device and intercepted password hashes can be cracked offline.

This MitM attack was successful in the lab environment for the Egardia gateway, which communicates every 10 seconds with a cloud service using basic authentication. The decoded Base64 string revealed the

```
▼ Hypertext Transfer Protocol
  ► POST /poll/sh HTTP/1.1\r\n
  ▼ Authorization: Basic c3Bl...g4M2U=\r\n
    Credentials: s...f:e1...ie
    Host: sh.egardia.com\r\n
```

Figure 41: Basic authentication used by Egardia

Egardia username and MD 5 password hash. Which turns out to be the exact username and password of the registered user account at Egardia.

The basic authentication string is automatically decoded by Wireshark into the username and MD5 password hash. The username and password turned out to be the Egardia's username and password that were entered during registration of the alarm system. These harvested credentials can be used directly on the Egardia portal and provide complete control over the alarm system, including turning it on and off at any given time.

The adversary could get the target's address for example through social engineering and/or reconnaissance applications, such as Maltego<sup>15</sup> and Shodan<sup>16</sup>, and searching on social media sites.

Although the consequences of attacks on an individual lighting system is limited to the discomfort and annoyance of the owner. More importantly, it shows that the technology used for IoT devices can be misused by others. Especially security related products such as the Egardia system could give a false sense of security and safety to its users.

<sup>15</sup> <https://www.paterva.com/web7/> - Software used for open-source intelligence and forensics

<sup>16</sup> <https://www.shodan.io> - A search engine for Internet-connected devices

## Appendix B: Philips Hue Bridge Internal Debugger

### Creating usernames (Tokens)

When usernames are created on the HUE Bridge, the bridge transmits username in clear text over the network.

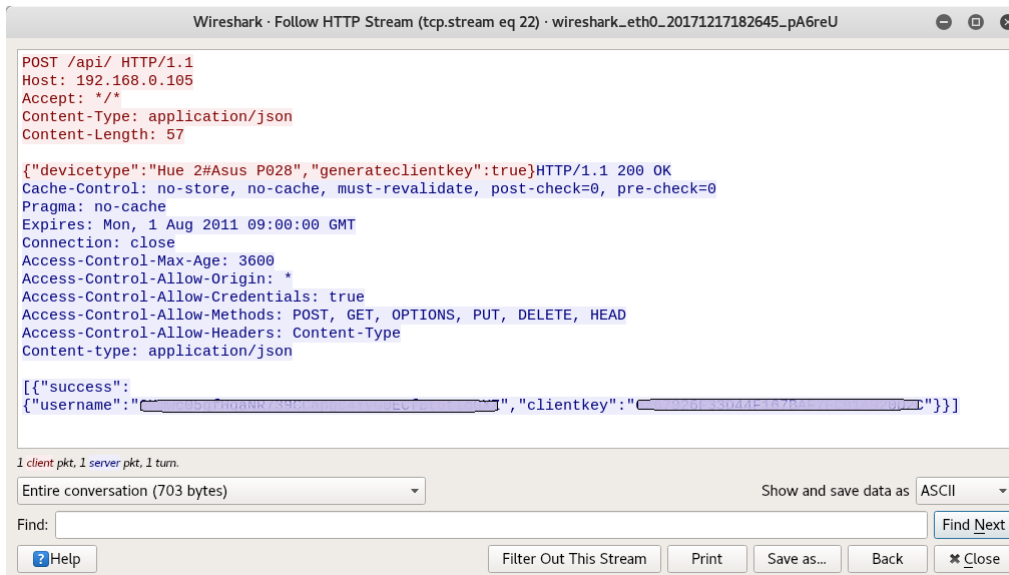


Figure 42: Transmission of clear text username (token) when installing an app

### Using the bridge’s APIs to create usernames

Each bridge has an internal debugger that can also be used to call the APIs including the creation of a username. The example below shows how this is achieved.

Launch Clip on <http://<ip-address>/debug/clip.html> and create a message body as shown in the figure below: {"devicetype": "<Some Name>", "generateclientkey": true}

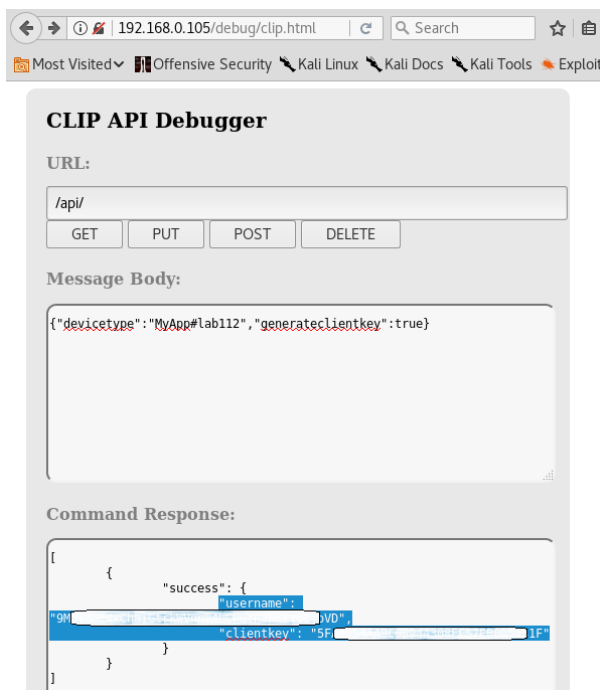


Figure 43: Whitelist of usernames (tokens) on the Hue Bridge

This generates a JSON output after physically pressing the button on the bridge or use another API to press the button “remotely”. This can be achieved by opening a second CLPI API Debugger as shown on the left with following settings:

1. URL: /api/<username>/config
2. Message Body: {"linkbutton": true}
3. and press “PUT”.
4. Then press “POST” again in the first debugger.

When the username is created successfully the output will be as shown on the left.

Now the new username can be used in the API Debugger to configure the bridge and operate the lights as described in the developer guides [76]. The config including the whitelist (authorized IDs can be retrieved from the bridge by using the following URL: <http://<bridge-ip-address>/api/<username>/config>

**Viewing the devices' location:**

**URL:**

/api/w7aF94yqQLZ3NPiudlevdiZ3oOJFk7LFuHBhpgu/sensors

GET PUT POST DELETE

**Message Body:**

**Command Response:**

```

    "modelid": "HA_GEOFENCE",
    "manufacturername":
"9sKysM0o7DWJDeJ9VKbR6KMu74rTvCJ0",
    "swversion": "A_1",
    "uniqueid": "L_02_CoRoX",
    "recycle": true
  },
  "8": {
    "state": {
      "presence": false,
      "lastupdated": "2018-01-21T12:25:36"
    },
    "config": {
      "on": true,
      "reachable": true
    },
    "name": "Asus P00C",
    "type": "Geofence",
    "modelid": "HA_GEOFENCE",
    "manufacturername":
"w7aF94yqQLZ3NPiudlevdiZ3oOJFk7L",
    "swversion": "A_1",
    "uniqueid": "L_02_YqCQX",
    "recycle": true
  }
}
    
```

Figure 44: Obtaining device location information from the bridge

# Appendix C: Device information send to data.flurry.com by Philips Hue

Burp Suite Community Edition v1.7.30 - Temporary Project

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension
125	https://data.flurry.com	POST	/aap.do	✓					do
124	https://data.flurry.com	POST	/aap.do	✓					do
123	https://data.flurry.com	POST	/aap.do	✓					do
122	https://data.flurry.com	POST	/aap.do	✓					do
121	https://data.flurry.com	POST	/aap.do	✓					do
120	http://172.217.20.110	GET	/generate_204			204	102		

Request

Raw Params Headers Hex

```

POST /aap.do HTTP/1.1
Content-Type: application/octet-stream
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.4.4; Samsung Galaxy S4 - 4.4.4 - API 19 - 1080x1920 Build/KTU84P)
Host: data.flurry.com
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 4196

!0p0`Y=ü 08JJTRZ68VFK3N2T83Y3Y02.18.0055070000dMYp8L657'mU:rss0AND8e977b3elaadaf73
fb990a588-58f9-41a3-9aef-b6e7077a51d1000`zUsa0`Y=|;000device.model.Samsung Galaxy S4 - 4.4.4 - API 19 -
1080x19200build.brand.generic0build.id0KTU84P0version.release04.4.40build.device0vbox86p
build.product0vbox86p0proguard.build.uid0android.intent.extra.REFERRE00https://account.meethue.com/get-token/?client_id=U0fV0crcV:mn
bHSe1H9alBzPBN15YN&response_type=code&state=TtGH&deviceName=Genymotion%20Samsung%20&appid=hue_android_app&deviceid=764f7a3675414a4a1
59616968556c4f"com.android.browser.application_id0com.android.chrome
org.chromium.chrome.browser.eem0[]'org.chromium.chrome.browser.referrer_id0com.philips.lighting.hue002.18.0080002000`Y=|;Rv0000b
attery.remaining.start01.00carrier.name0Android0memory.available.start
16957849600battery.remaining.end01.00disk.size.total.internal03902550battery.charging.start0true0battery.charging.end0true0disk.size.to
tal.external011159250memory.total.start
16957849600disk.size.available.external011159250memory.total.end
1691574272 boot.time15145000290000memory.available.end
16915742720carrier.details03102600disk.size.available.internal03902550en_US0Europe/Amsterdam009001788FFFE47B50D,2lsyuijgdVPt5T-c6KAu5u
uxxPHlglfZH17jdTWHYyy00More_Login_LoginButton00Developer_Authentication_Event0,Developer_Bridge_Identifier_Remove_Whitelist00Connection_
Connecting00HomeDashboard_More00Connection_Status0000HomeDashboard_More00Rr00More_Login_LoginButton0
ErrorCode0SUCCESS0result0success0AP000Connection_Connecting0*000Connection_Connecting0`0,Developer_Bridge_Identifier_Remove_Whitelist
0bridgeIs_Null0false0BridgeHasIdentifier0true0-0,Developer_Bridge_Identifier_Remove_Whitelist0
bridgeIs_Null0false0BridgeHasIdentifier0true0-00Developer_Authentication_Event00hasBridgeConfig0true0hasBridgeVersion0true0event
AUTHENTICATED00,Developer_Bridge_Identifier_Remove_Whitelist0bridgeIs_Null0false0BridgeHasIdentifier0true00
0Connection_Status00Type0remote00
,Developer_Bridge_Identifier_Remove_Whitelist0
bridgeIs_Null0false0BridgeHasIdentifier0true0!0,Developer_Bridge_Identifier_Remove_Whitelist0
bridgeIs_Null0false0BridgeHasIdentifier0true0C00Connection_Connecting00result0success0J0u,Developer_Bridge_Identifier_Remove_Whitelist0
bridgeIs_Null0false0BridgeHasIdentifier0true0MD,Developer_Bridge_Identifier_Remove_Whitelist0
bridgeIs_Null0false0BridgeHasIdentifier0true0PD,Developer_Bridge_Identifier_Remove_Whitelist0
bridgeIs_Null0false0BridgeHasIdentifier0true0I00Connection_Status00Type0Offline00,Developer_Bridge_Identifier_Remove_Whitelist0
bridgeIs_Null0false0BridgeHasIdentifier0true000,Developer_Bridge_Identifier_Remove_Whitelist0
bridgeIs_Null0false0BridgeHasIdentifier0true000,Developer_Bridge_Identifier_Remove_Whitelist0
bridgeIs_Null0false0BridgeHasIdentifier0true0a00Developer_Authentication_Event00hasBridgeConfig0true0hasBridgeVersion0true0event
AUTHENTICATED00,Developer_Bridge_Identifier_Remove_Whitelist0
bridgeIs_Null0false0BridgeHasIdentifier0true0M00Connection_Status00Type0remote0;0,Developer_Bridge_Identifier_Remove_Whitelist0
bridgeIs_Null0false0BridgeHasIdentifier0true0A00Connection_Connecting00
00Connection_Connecting0^300,Developer_Bridge_Identifier_Remove_Whitelist0
bridgeIs_Null0false0BridgeHasIdentifier0true0600Connection_Connecting00result0success0600,Developer_Bridge_Identifier_Remove_Whitelist
0bridgeIs_Null0false0BridgeHasIdentifier0true0600AAA
    
```

0 matches

