Master thesis
Security Risk Assessment of LoRaWan

Vojtech Brtnik
vojtech@brtnik.eu

January 2018

CYBER
SECUR
ITYAC
ADEMY

Master Thesis

Executive program Master of Science (MSc) Cyber Security
Cyber Security Academy The Hague (CSA)
Leiden University

Student: Vojtech Brtnik, nr. s1789856
Supervisors: Carlos H. Gañán, J.C.A. van der Lubbe

Date of defense: 25 January 2017

Abstract

The subject of study is security in the LoRaWan protocol version 1.0.2 class A. The thesis looks at the subject on behalf of the manufacturers and consumers and asks what the security risks in the protocol are when used in consumer products, and what should be done about them. We answer the question in two phases: by first studying the existing academic and industry results, summarizing known threats, vulnerabilities and countermeasures in the protocol. This provides a novel risk assessment of the protocol on its own. In the second phase, using the results of the first phase, we conduct a qualitative research in the form of expert semi-structured interviews where context is provided to these initial results. The thesis concludes that the LoRaWan comes with many inherent security weaknesses that can be expected given the functional requirements with which the protocol was designed. These weaknesses need to be taken into consideration by manufacturers adopting the protocol in their solution. We list which use cases are suitable for the protocol and which use cases should be avoided by manufacturers and consumers. We further state 4 principles that should be adopted by manufacturers when adopting LoRaWan into their products, along with attention points for other stakeholder groups.

Acknowledgements

I would like to thank all those experts that took part in the interviews and endless discussions on various topics, willing to share their opinions and experience.

A big thank you also goes to my girlfriend Kana for her continuous love and support including during the many weekends, late evenings, and holidays that I paid more attention to the thesis than to her.

This thesis concluded a two yearlong study at the Cyber Security Academy at Leiden University. This was a great time of my life, especially because of the people involved: the professors, guest lecturers, faculty staff, as well as fellow students. Especially I would like to thank my supervisors Carlos Gañán and Jan van der Lubbe for their guidance.

Table of Contents

1 Introduction and Problem Statement 4

2 Scope and Context of the Thesis 5

3 Research Methodology and Scientific Contribution 12

4 Phase 1: Desktop research - Security Risk Assessment of LoRaWan connected Consumer Products 21

5 Phase 2: Stakeholder Interviews 43

6 Synthesis and Discussion 60

7 List of tables and figures 63

8 Works Cited 64

1 Introduction and Problem Statement

Most of us will agree that the connected world is a concept that will transform the world in the years to come. In fact, the transformation already began in many geographies, industries and societies. The transformation has been enabled by exponential technological developments in many areas. One such relatively recent innovation is a class of LPWAN technologies (low power wide area networks) that can support low power connected devices over long range. One such technology is LoRaWan. Multiple states deployed LoRaWan country-wide and various applications quickly emerged.

As most of us believe in this technological progress, we have also learnt in the past that keeping the new technologies and newly created (cyber) space secure for everyone is a difficult task. Ever since history remembers people have valued safety and security for themselves, their societies and their possessions, they wanted to preserve their privacy, and feel secure. The connected world is no different.

This research is directed at the world of consumers and connected device manufacturers in the LoRaWan environment. There has been a lot written about individual aspects of LoRaWan and individual aspects of its security. But none of that research asks the question: So what? No comprehensive research aimed at consumers and device manufacturers has been done. This research aims to close the gap and strives to help consumers and device manufacturers answer whether they can trust the LoRaWan connected world and feel safe, secure, and comfortable.

We state the following research problem: What are the cyber security risks for consumers and manufacturers in the world of LoRaWan-connected internet of things (IOT) consumer products and what can be done about it?

The thesis is structured as follows: Chapter 2 provides wider introduction into the problem and its context. Chapter 3 explains the research methodology. The thesis follows two-phase approach. We first study existing academic and industry results, summarizing known threats, vulnerabilities and countermeasures in the protocol. In the second phase, using the results of the first phase, we conduct a qualitative research in the form of expert interviews where context is provided to these initial results. The first phase - theoretical research - is subject of Chapter **Error! Reference source not found.**. The expert interviews are subject of Chapter **Error! Reference source not found.**. Chapter 6 provides conclusion, critically looks back at the thesis and summarizes the work.

2 Scope and Context of the Thesis

This section will introduce the reader to the IOT landscape and limit the scope of the research to cybersecurity-related aspects of the LoRaWan-connected consumer-grade IOT devices. See Figure 1.

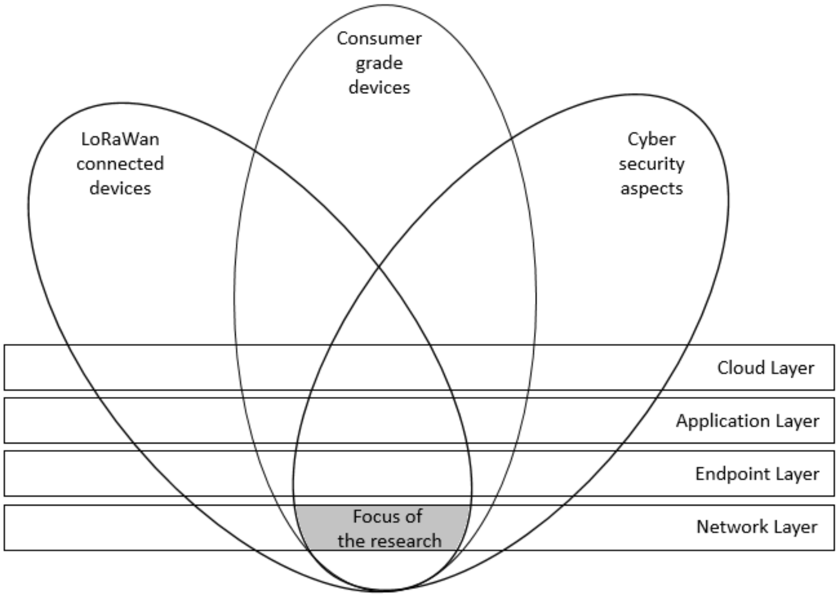

Figure 1: Focus of the research in context of the IOT ecosystem.

2.1 Introduction to the IOT landscape

Internet of things (hereinafter: IOT) is a relatively new concept. As a term, it was probably coined in 1999 by Kevin Ashton [1], but as a concept it started living long time before that. One could argue that the electromagnetic telegraph from the beginning of 19th century is its first application. Numerous definitions were created over time; the following paragraph summarizes some of them.

1) 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 (ITU).
2) A world-wide network of interconnected objects uniquely addressable, based on standard communication protocols (...) having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts [2].
3) Interconnection of physical objects, by equipping them with sensors, actuators and a means to connect to the Internet [3].
4) A wired or wireless network of uniquely identifiable connected devices which are able to process data and communicate with each other with or without human involvement [4].
5) A concept: anytime, anywhere and any media, resulting into sustained ratio between radio and man around 1:1 [5].

In this thesis, we will loosely follow the first definition, which stresses the concept of a connectivity (either virtual or physical) and the importance of data and information as a basis for smarter decisions.

Use cases for IOT are endless and well documented. Gartner predicts that by 2020, total 25 billion devices will be connected to the network, CISCO estimates 50 billion and European Commission between 50 and 100 billion devices [6].

IOT offers endless opportunities across different industries, from heavy manufacturing, to automotive, to critical societal services, all the way to connected homes and relatively simple end-user consumer products. These opportunities attract inexperienced start-ups as well as established enterprises wishing to innovate their portfolio. The below paragraphs should give the reader a sense of what possibilities the Internet of Things offer. It is not meant to be an exhaustive list, rather an illustrative list with further references for those interested.

Smart manufacturing. Automation in manufacturing has been discussed at least since 1980s. Today's factories are run more by computers than by humans, based on sensors connected to intelligent decision making units. Computers check the status of the supply chain, conditions in the factory, and real-time customer demands and adjust the factory processes. Smart manufacturing utilizes the concepts of the cyber-physical systems, internet of things (and everything), cloud computing, service oriented computing, artificial intelligence and data science. [7] According to Gartner, smart manufacturing will dominate the applications on the IOT market [8].

Automotive. The automotive industry is predicted to be among the fastest growing areas of the IOT market. Car manufacturers are already including or testing IOT related functionality such as fleet management and car GPS mapping; remote monitoring of the vehicle's performance by garage maintenance; monitoring engine efficiency; control of the vehicle's entertainment systems, heating, safety locks, or lights from mobile devices; and autonomous safety mechanisms such as self-steering, braking, or communication with emergency services. The car industry is moving towards becoming a mobile e-commerce platform and location based ads and driver profiling services are also emerging.

Critical Infrastructure are those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed have serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of the governments. Examples are electricity and gas facilities, water supplies and management, flight and airplane management, police and government services [9].   It is easy to imagine how smart sensors on the critical infrastructure and connection to the network could increase quality and efficiency of these networks. For example, a sensor measuring the quality of the water, and alerting real-time both government and citizens in case of contamination could save lives in case of a chemical terrorist attack. Connecting paramedic emergency units to the network would not only give hospitals a better overview of where these units are, but would also allow smoother better preparation for a handover of the patient. A hospital can tailor the preparation more precisely if the doctors know when the paramedic ambulance is arriving, what the characteristics and the diagnosis of the patient are, how his organs are functioning, what the composition of his blood is and what treatment he has been given prior to arrival to the hospital.

Smart Cities. Cities are considered smart when investments in human and societal capital, traditional infrastructure and disruptive technologies fuel sustainable economic growth and high quality of life, with a wise management of natural resources, and thought participatory government. According to a Deloitte study, smart cities are not an isolated phenomenon but part of a transition towards digital economy [10]. The smart cities market, made up of interrelated domains is expected to reach USD 1.15 trillion by 2020, driven by tech innovation [11].

Connected Homes. As electronic sensors are getting smaller, lighter, more portable, and cheaper to manufacture, they are being included into more and more home consumer products such as kitchen appliances, home entertainment systems, lightning, safety mechanisms,

Consumer products (business to consumer market): products built by industries for end-users, such as geo-tracking devices, fitness and smart watches, calories intake tracker, and sleep quality trackers.

The scope of this thesis is limited to consumer products. The reasoning behind the choice is explained in the next section.

2.2 Challenge with Consumer Products

We limit the scope of the research to consumer products. This section explains why.

Typical consumers have little influence over the quality of the product they buy, its end-user license agreements, and nonfunctional specifications (such as privacy and security). Furthermore, they often do not have enough skills to differentiate a product which is built with security and privacy in mind from a product that is only focusing on the core functionality and look and feel. This creates a lemon market in which developers and manufacturers do not have enough incentives to invest into privacy and security.

The market for consumer products is growing, and prices are falling. Often, the main deciding factor whether a new product will succeed on the market is time. Start-ups as well as established manufacturers are racing to be the first on the market with each new technology and feature.

Combining the above two facts together, we may assume that security of consumer products is not high on the priority for either the consumer or the manufacturer.

The large players on the business to business market have purchasing departments usually with enough power and skills to negotiate specific functionality, license agreements, and quality of the final product. Large companies also have strict policies in place for security, and are able to deploy additional measures such as firewalls, threat management and monitoring systems to compensate for the potential lack of security in the IOT products.

On the other hand, large enterprises are more attractive targets to high profile criminals such as nation states and organized groups who are able to develop advanced cyber weapons and invest sufficient resources to overcome multiple countermeasures.

To conclude this section, it can be stated with fair amount of certainty that no one connected to the network can be 100% sure of its security. In order to keep the research scope limited, we have decided to focus on consumer products on the B2C market.

The next section will further elaborate why cyber security of IOT devices is a relevant, but often forgotten concern.

2.3 Cyber Security for IOT Consumer Products

This section explains why cyber security is a relevant topic to study for IOT consumer products.

This section presents four points: (a) IOT as a technology is still fighting for proving its value and focus is on that; (b) managing risks and especially security risks will become very important; (c) network connectivity will play a key role in ensuring security of the IOT systems; (d) prescribing and testing security will be the safeguard.

According to the Gartner Hype Cycle for Emerging Technology in 2017, IOT platforms are reaching the peak of inflated expectations [12]. This phase is characterized by over enthusiasm and inflated expectations, and focus is more on added value business cases than on identifying and managing risks. As the technology will go through the cycle phases of disillusionment, enlightenment, and is expected to reach plateau of productivity in 2-5 years, there will be an increasing focus on managing the risks and challenges. We still have a lot to learn about the risks and challenges in IOT systems. The highest known risks are in the area of safety and security & cyber.

When it comes to safety, we know about risks related to injuries and traffic accidents caused by malfunctioning safe-driving cars, as well as risks to property theft and damage.

Earlier this year, Uber suspended the self-driving car program following a car crash of one of the test driverless cars [13]. In 2016 a man was killed in Florida highway when using a self-driving autopilot in a semi-autonomous driving car [14]. Especially important risks will be those connected to actions by malicious parties and criminals. Cyber attack on a factory mill in Germany is known to have caused programming error in the steel furnace, which thereafter exploded and caused a physical damage of the property [15]. Chrysler had to update software in their cars after researches demonstrated how to stop the engine and take control of the car's steering and breaking system via the IOT entertainment system [16]. Another research showed how to access home network and steal usernames and passwords through vulnerabilities in the network connected light bulb system [17].

Already now, ensuring that the IOT ecosystem is secure and privacy-friendly by design is seen as one of the most significant challenges for designers, entrepreneurs and engineers alike. For example, the IOT Design Manifesto drafted by professionals working in the IOT field lists 10 principles for developing IOT products. Principle IV states that "we keep everyone and everything secure" and principle V states that "we build and promote a culture of privacy" [18].

The following 3 examples will demonstrate how lack of security in IOT devices can lead to risks:

- Case 1 (Dyn attack): In October 2016, a large DDOS attack was targeted at Dyn, a US internet service provider, which controls much of the Internet's DNS infrastructure. A big part of the Internet in US was not reachable including sites of CNN, Twitter, Netflix. The attack was executed using the Mirai botnet. The botnet consisted of more than 100 thousand consumer IOT devices such as digital cameras and DVD players infected by malware. The attack classified as a largest of its kind in the history [19].
- Case 2 (Fitbit hack): In January 2016, accounts of Fitbit, a manufacturer of smart consumer wearables, were hacked. The attack affected those reusing usernames and passwords across the Internet. The hack gave attackers access to user's personal data, lifestyle, daily activity, and potentially GPS coordinates in the past. The attackers monetized the hack by ordering replacement items, under the Fitbit's warranty policy via the hacked accounts [20], and then selling them back to the market in exchange for money, thus making profit.
- Case 3 (Motion sensor hack): Research showed that data from motion sensors of a mobile phone can be used to infer keystrokes entered on its touch screens [21] [22]. Recently, researchers also identified a way in which data from gyroscopes and accelerometer sensors embedded in smart watches can be used to guess which PIN code does a user enter on a PIN pad provided. These sensors will capture the movement of the hand when entering the PIN code. Researchers showed that it is possible to extrapolate the PIN with a large degree of probability [23].

IOT sensors are often simple, low-cost and low-power devices. A different approach for securing these must be taken than for securing traditional server-side or end-user computers. For traditional devices computational power and disk storage has become widely available, and deploying a whole security suite consisting of firewalls, anti-malware devices, and monitoring and detection software is commonplace. Low-cost IOT devices often will not have the capacity to run such software stack and much of the security burden will fall on the network and communication protocol itself. A number of network technologies are currently competing to become the standard for network connectivity for IOT. These are further discussed in the next section. However, for the aforementioned reasons, all of them are expected to provide security out of the box.

In general, two main approaches to providing security exist. A prescriptive approach whereby the focus is on ensuring that a system is designed securely with controls in place to preventing every possible form of vulnerability or failure, as well as threats from exploiting the system. However, the IOT systems are too complex for anyone to analyze and predict all possible scenarios. Therefore, prescriptive approach is complemented with a descriptive approach and end-to-end testing of the systems. With systems modeled accurately in laboratory conditions, testing is a safe way of simulating unwanted conditions such as hardware or software failures, malicious parties interfering with the system, or unexpected scenarios and edge conditions occurring that were not thought of by the designers of the system. Testing of ICT systems is a well understood process with existing methodologies and proven benefits. Although IOT as such will add various complexities (such as new network protocols, new threats and countermeasures, and different hardware and software architecture of the solutions), the basic testing principles remain the same and can be re-used.

In conclusion, this section argued that although current main focus in the IOT community is on demonstrating the usefulness of the technology, managing risks is equally important. Due to the nature of IOT devices, security of the network connectivity will play a key role. Due to the complexity of the IOT ecosystem, it is not possible to prescriptively analyze and predict all risks, and security testing will be an important step.

This thesis will focus on cyber security topics related to consumer-grade IOT endpoint products.

2.4 Introduction to Networks for IOT and Specifically LoRaWan

This section introduces the main object of this research: the network layer, and the LoRaWan protocol. The focus of this thesis is the version 1.0.2 of this protocol communication class A only.

A number of network protocols were developed over the past to support data transfer for IOT devices. They differ in the maximum data capacity, distance they can cover, number of devices they support, availability of the technology across different geographies, scalability, or price to adopt them on the market.

The following list summarizes some of the most commonly available technologies, and their advantages and disadvantages:

Low Energy Bluetooth (BLE) is cheap and offers a long battery life, low energy consumption, high data rates (1 Mbps), and in theory unlimited number of supported devices. The main disadvantage are a limited range (max. 50 meters) and the need for central access point to link back to the network.

ZigBee (802.15.4e) is a low cost implementation protocol operating in unlicensed frequency band that supports large number of devices (up to 65000), low power consumption, but is also limited in range (max. 100m) and data rate (250 kbps).

IEEE 802.11ah amends the existing Wi-Fi specification (IEEE 802.11) to support IOT devices. Wi-Fi is a well-established protocol available almost everywhere, based on a cheap infrastructure, also operating in the unlicensed frequency band. 802.11ah can reach very high data rates (up to 346 Mbps) for up to 8000 devices, has medium range coverage (up to 1.5 km) and offers relatively low power consumption.

Cellular data (3G, 4G) is another protocol available almost everywhere. Disadvantage is that it operates in a licensed frequency band, uses a lot of battery power, and is based on expensive hardware, and incurs network charges.

This research will limit itself on LoRaWan. Reason for this is that LoRaWan became very popular in the Netherlands and is an ideal technology for low-data traffic devices operating over large ranges, which covers many consumer grade IOT products.

LoRaWan is a Low Power Wide Area Network (LPWAN) intended for wireless battery operated Things in a regional, national or global network [24].   LoRa is a network based on an open standard LoRaWan. LoRa uses an unlicensed spectrum, with different bands per country. LoRa is not a very fast protocol, maximum rate for short ranges is around 50kbits/second, and around 292 bits/second for larger ranges. LoRa can reach up to kilometers, and can also penetrate obstacles that would stop other networks.

In the Netherlands LoRaWan network was first launched in November 2015, and as of June 2016 is accessible across the Dutch market. KPN is one of the infrastructure service providers for the network [25].

LoRaWan is therefore designed for long-range, low-data connections, low-power operations with sensors that are operating on batteries with limited charging possibilities. Thanks LPWAN technologies, IOT devices operated by batteries can last in many cases months before the battery is depleted. LPWAN thus offers a low-cost, low-consumption and low-energy alternative to 3G and 4G networks. This opens a new business model, in which low-cost IOT devices can be offered to in a user-friendly manner, without the need of frequent battery charging.

The following list presents a number of existing consumer grade IOT products on the market that make use of the LoRaWan network.

- GeoWAN Cattle Tracking is a monitoring LoRaWan-based IOT device for Australian farmers. In order for a farmer in Australia to enter a business, he initially invests a large amount and purchase the cattle. This investment needs to be insured, since cattle frequently gets lost. In order for the farmers to reduce the risk, and thus reduce the insurance premium, they can use GeoWAN which allows to track via the Internet the location of the cattle [26].
- xignal Mousetrap is a LoRaWan-connected mouse trap that allows home owners to monitor via a mobile application whether a mouse has been caught by the trap, or not, or even whether the mouse has been clever enough to eat the bait while avoiding to be caught [27].
- Auroras LoRaWan sensors for doors and windows can be used to enhance the home monitoring burglar alarm system. In case that the sensors notice movement, they sent a signal to the central server which raises an alarm. The importance of this use case is that it that correct and secure working of the system has direct influence on physical safety of the property, and in some cases also the people within the monitored environment.
- ioTracker is a key chain IOT device. The main use case for ioTracker is locating devices that can be misplaced or lost such as e.g. a bicycle or wallet. Using the LoRaWan network the device communicates with the ioTracker backend server and exchanges location data. End user has then access to the functionality offered by ioTracker via a web-based or mobile-app dashboards. The location tracking using

the LoRaWan signal works on a triangulation basis. The device sends in the regular intervals LoRaWan signal to its surrounding. The gateways operated by the network operator will receive the signal and inform the server about which gateway received the signal and when. The server will triangulate the information and calculate the location of the device.

2.5 IOT Security Architecture

This section will build up further the notion of cyber security for IOT devices, and explain the model used in this thesis.

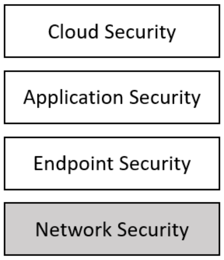

Figure 2: Model for IOT security architecture with the focus area highlighted

In order to study the security of the IOT landscape, we will first look at the architecture of the landscape with relation to security, and from which components it is built up.

Depending on the abstraction layer, different categorization angles exist. The following paragraph summarizes some of the existing views on the IoT architecture from the existing literature, and demonstrates the various angles that one can take.

- Gartner in its report on IOT security looks at the landscape from a purely technological perspective and identifies the following domains: network security, endpoint security, application security, cloud security and others [8]. In the same report Gartner states that network security is one of the most important aspects of the IOT ecosystem, and that the capability is expected to hold the largest market share in the IOT security market [8]. The disadvantage of this view is that it says very little about the cyber activities and cyber actors that take place in the IOT landscape.
- O'Neill distinguishes between (a) the IOT devices themselves - the sensors, (b) the communication layer, and (c) the backend systems that store and analyze the data generated by the sensors [28]. This is a very similar view to the one of Gartner, closer to the way that the devices are operating in the physical world. Mapping the two on each other, network security represents the communication layer, endpoint security the IOT devices, application security and cloud security the backend systems.
- Ray identifies 6 functional blocks: device, communication, services, management, security, and application [29]. Security is viewed here as a separate functional block, rather than an essential requirement that all components of the IOT landscape should implement.
- Abomhara and Koien identify IoT devices and IoT services [30]. IoT device are the hardware components, and IoT services offer the functionality and enable interaction between entities. This view of splitting the domain into software and hardware is too superficial and not detailed enough for most applications.

We will adopt the classification of Gartner [8], also see Figure 2. The scope of the thesis will be limited to cyber related risks to consumer products for the network security.

3 Research Methodology and Scientific Contribution

The thesis follows two-phase approach. In the first phase, we first study existing academic and industry results, summarizing known threats, vulnerabilities (incl. threat actors) and mitigating countermeasures in the LoRaWan version 1.0.2 class A protocol. In the second phase, using the results of the first phase, we conduct a qualitative research in the form of expert interviews where context is provided to these initial results. Refer to Figure 3: High level process.

As a reminder, the use case considered in the thesis is a consumer-grade lightweight IOT device communicating over LoRaWan network. We are only considering those cyber security threats, counter-measures and vulnerabilities that are related to the LoRaWan network communication. Other aspects, and specifically including broader privacy-related questions, are out of scope. Refer to Chapter 1 for further details.

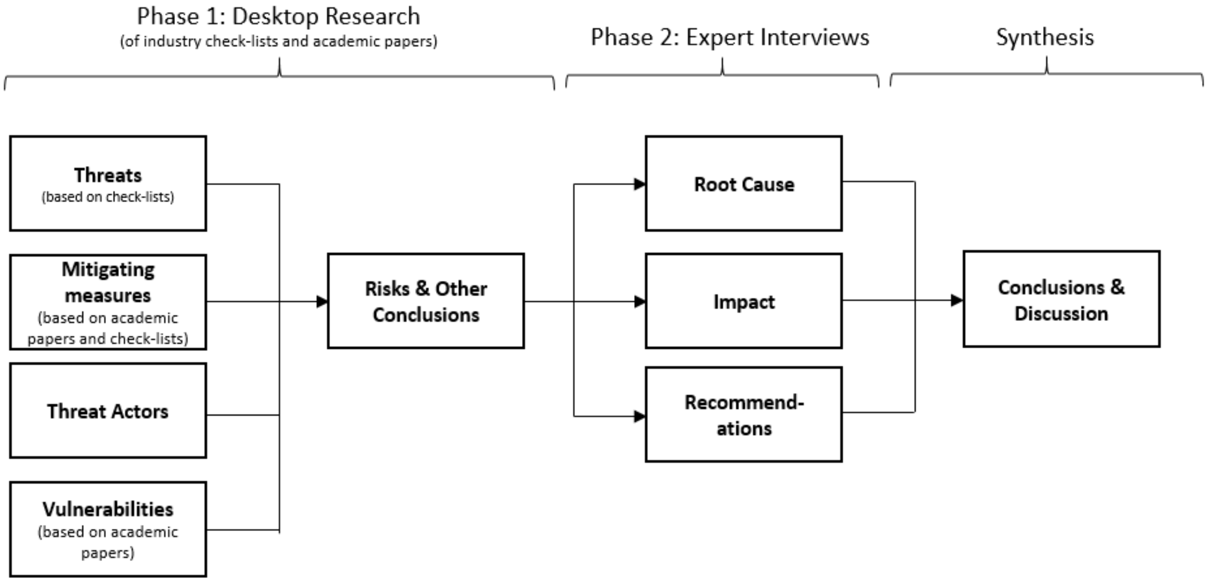
Phase 1: Desktop Research
(of industry check-lists and academic papers)
Phase 2: Expert Interviews
Synthesis
Threats
(based on check-lists)
Mitigating measures
(based on academic papers and check-lists)
Threat Actors
Vulnerabilities
(based on academic papers)
Risks & Other Conclusions
Root Cause
Impact
Recommend-ations
Conclusions & Discussion

Figure 3: High level process

3.1 Phase 1: Desktop research

The first part of the thesis consists of a desktop research and consolidation of known threats, vulnerabilities, and mitigating measures relevant for LoRaWan version 1.0.2 class A protocol. The research follows by a further described risk assessment methodology.

International standard ISO 31010:2009 Risk Management lists in the Annex B possible Risk Assessment Techniques. We follow a risk assessment techniques called check-lists described in the standard.

An input to this phase will be a list of frameworks, existing scientific literature, and internet articles.

The output of this phase will be a list of threats, vulnerabilities, and mitigating measures specific to network security and LoRaWan classified in a consistent theoretical framework. As far as known to the author, no similar consolidation and categorization of threats, vulnerabilities, and mitigating measures has been done to date for LoRaWan version 1.0.2 class A. Such a database will thus contribute to the scientific body of knowledge.

The detailed methodology for collecting threats, vulnerabilities, and mitigating measures is described in the consequent paragraphs.

3.1.1 Identifying threats and mitigating measures

The process for identifying threats and mitigating measures is depicted in Figure 4.

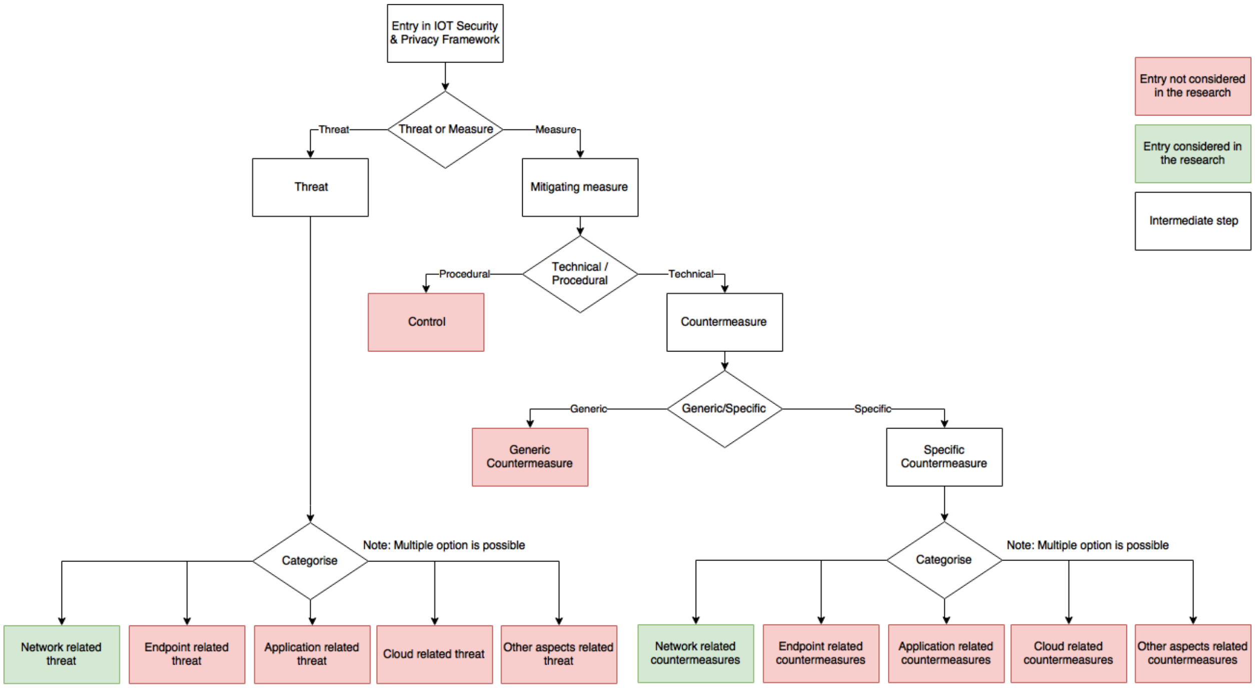
Entry in IOT Security & Privacy Framework
Threat or Measure
Threat
Measure
Threat
Mitigating measure
Technical / Procedural
Procedural
Technical
Control
Countermeasure
Generic/Specific
Generic
Specific
Generic Countermeasure
Specific Countermeasure
Categorise
Note: Multiple option is possible
Categorise
Note: Multiple option is possible
Network related threat
Endpoint related threat
Application related threat
Cloud related threat
Other aspects related threat
Network related countermeasures
Endpoint related countermeasures
Application related countermeasures
Cloud related countermeasures
Other aspects related countermeasures
Entry not considered in the research
Entry considered in the research
Intermediate step

Figure 4: Core part of the process for consolidating known and relevant threats and mitigating measures.

To arrive at known threats and mitigating measures, we gather the list of existing security and privacy guidelines (check-lists) for the Internet of Things. These include guidelines published by independent researchers, engineering working groups, and enterprise. Each guideline is rated with regards to applicability for the studied use case. Not applicable guidelines are not further considered. From the remaining guidelines, we extract the list of cyber security threats and mitigating measures. For the guidelines in scope of the research, we extracted the list of cyber security threats, controls and countermeasures.

In order to filter out applicable threats, controls and countermeasures, we classified the entries in the guidelines into the following categories. The categorization was selected based on the Gartner article [8]. Choice is discussed in Section 2.3.

- **Network Security**: threats, controls and countermeasures that address security of the network communication. This includes topics such as encryption and configuration of the network communication, authentication to the network, and logging and reliability of the communication.
- **Endpoint Security**: threats, controls and countermeasures specific to the physical computing devices that are interfacing with the physical world. In the considered use case for consumer products, these are typically the sensors, or simple physical devices that are connected to the LoRaWan network, and providing metrics via the cloud environment to the owner of the device. In this category the following

groups of threats or recommendations will be included: physical security of the endpoint, security of the firmware, security of the operating system running on the end point, configuration of the endpoint device, authentication to the device itself and the operating system of the device (not to the applications running on the device).

- **Application Security**: threats, controls and countermeasures specific to the application and software running on the IOT endpoint. This is typically the software created by the manufacturer of the IOT service. The software receives input from the endpoint sensors, performs a very limited calculation and sends the results over the LoRaWan network to the cloud environment.
- **Cloud Security**: threats, controls and countermeasures related to the environment beyond the endpoint and the LoRaWan network. These are typically more traditional IT environments, such as servers, and other backend and network systems, and service architecture. Web and mobile applications are also included in this category.
- **Other**: Any other threats, controls and countermeasures that could not be classified using one of the above categories.

In parallel with the above classification, we also categorized controls and countermeasures with one of the following three labels: procedural controls, technical generic countermeasures, or technical specific countermeasures.

- **Procedural controls**: with this tag we classify mitigation recommendation that are procedural in nature. These are typically guidelines that instruct owners, designers, developers, manufacturers, or other stakeholders what process should be followed when developing the IOT product or service, but not necessarily how the final product should look like, and what specific steps the stakeholder should follow to secure the final product. Examples of procedural countermeasures are "Perform threat modeling", "Provide a secure update facility", or "Ensure all IoT devices and associated software have been subjected to rigorous, standardized software development lifecycle testing".
- **Technical generic countermeasures**: these are countermeasures that are technical enough to give the reader specific instructions and content about what mitigation should be deployed. Generic counter measures are however still very high level to give detailed instructions about how the recommendation should be applied. Generic counter measures are often prescriptive in nature. Another downside of generic countermeasures is that they often do not consider the technical feasibility of the recommendation. Examples are "Incorporate Trusted Platform Modules into the IOT device", "Secure Physical Interfaces", or "Protect the device from physical perspective".
- **Technical specific countermeasures**: these are countermeasures that are technical and specific enough to be actionable and instructive about what mitigation should be deployed. Specific countermeasures are often descriptive rather than prescriptive. The disadvantage is that they might be very specific to a certain situation and not applicable for all use cases and scenarios. Examples are "Implement Certificate Pinning Support within IOT firmware", "The protocol includes functionality to detect if all or part of a message is an unauthorized repeat of an earlier message or part of a message.", or "Ensure all devices operate with a minimal number of network ports active".

A known limitation of the above classification is its subjectivity. The mentioned categories are not defined exactly and it is possible that other researches and subject matter experts would categories some of the threats or recommendations differently. The categorization was done on a consensus basis in a group of subject matter experts, and discussion was held for disputable items. Similarly the borderline between what is a procedural control, generic technical countermeasure and technical countermeasure is somewhat blurry. However, the categorization was necessary to further focus the research on most relevant and specific threats and countermeasures for the use case of this thesis. This is further discussed in the next section.

The research considers only technical counter-measures that are applicable for network security. These are further grouped together, with duplicities removed. The remaining is the resulting list of cybersecurity threats and specific technical counter-measures that should be applied in the considered use case.

3.1.2 Identifying threat actors and vulnerabilities

Known vulnerabilities are collected by consolidating existing results of laboratory vulnerability testing, and original theoretical vulnerability desktop research that focus specifically on LoRaWan and IOT.

The reason for deviating from the process for collecting threats and mitigating measures is that we did not discover any check-lists that contain a list of vulnerabilities applicable to LoRaWan version 1.0.2. class A. Vulnerability databases such as CWE or CVE do not contain any relevant entries, and the encountered framework did not discuss vulnerabilities.

By definition, each considered vulnerability is network-related and specific enough to be considered in further research.

3.2 Phase 2: Stakeholder Interviews

This paragraph describes the process and methodology for conducting expert interviews. The high level process is described in Figure 5.

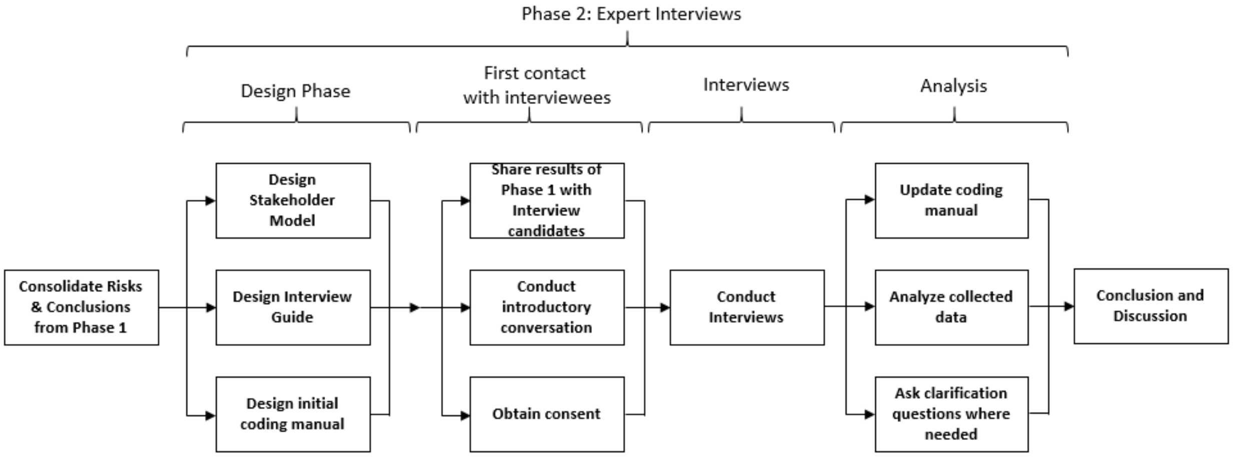
Phase 2: Expert Interviews
Design Phase
First contact with interviewees
Interviews
Analysis
Consolidate Risks & Conclusions from Phase 1
Design Stakeholder Model
Design Interview Guide
Design initial coding manual
Share results of Phase 1 with Interview candidates
Conduct introductory conversation
Obtain consent
Conduct Interviews
Update coding manual
Analyze collected data
Ask clarification questions where needed
Conclusion and Discussion

Figure 5: High level process for expert interviews

3.2.1 Context to the qualitative research

The first phase of the thesis research, which took form of a desktop research conclude a number of facts. In the second phase, to provide context to those facts, a qualitative study was conducted. The study addressed the following questions related to the above conclusions.

1) **Root cause**: How do you explain the conclusions from phase 1?
2) **Impact**: What impact does that have on various stakeholders, and primarily consumers and manufacturers?
3) **Recommendation**: Should we do something about it and what?

3.2.2 Qualitative Research Methodology Summary

A qualitative study was conducted to provide context to the outcome of the desktop research.

Data was collected by means of interactive individual in-depth semi-structured interviews with experts and consumers. Stakeholders were selected for the interviews based on a stakeholder framework for IOT LoRaWan consumer product ecosystem. An interview guide was created to cover the main research questions. Most interviews were voice recorded and typed in a text document for later analysis, some interviews were conducted via email. Each participant was informed about the purpose of the research, and gave an informed consent with participation and the process either via email or verbally before the interview.

Descriptive coding was used to analyze the collected data. The reason for choosing descriptive coding is that the primary goal of the interviews was to understand subjective opinions of stakeholder representatives of the IOT LoRaWan ecosystem in order to explain root cause, impact, and recommendations related to the outcomes of the desktop research.

The methodology is further elaborated in the following sections.

3.2.3 Stakeholder Model

In order to collect a balanced data set from the interviews, a stakeholder model is created. Based on this model, experts were approached for interviews. The stakeholder landscape was split into a number of groups. The aim of the research was to collect input from representatives of as many groups as possible.

In general, we split the stakeholder landscape around IOT Consumer Products into the following 3 groups:

1) Specific LoRaWan Ecosystem Stakeholders
2) Consumers
3) LoRaWan-related but Generic IOT & IT Ecosystem Stakeholders

The world is one interconnected ecosystem and in order to conduct a meaningful research, one has to draw a border around the scope. In this research, we will consider only groups 1 and 2 for the interviews. Group 3 is very general, and their actions and opinions have a lesser degree of influence on the security of the LoRaWan IOT ecosystem. Group 1 is further split into a number of stakeholder categories, as depicted in Figure 6.

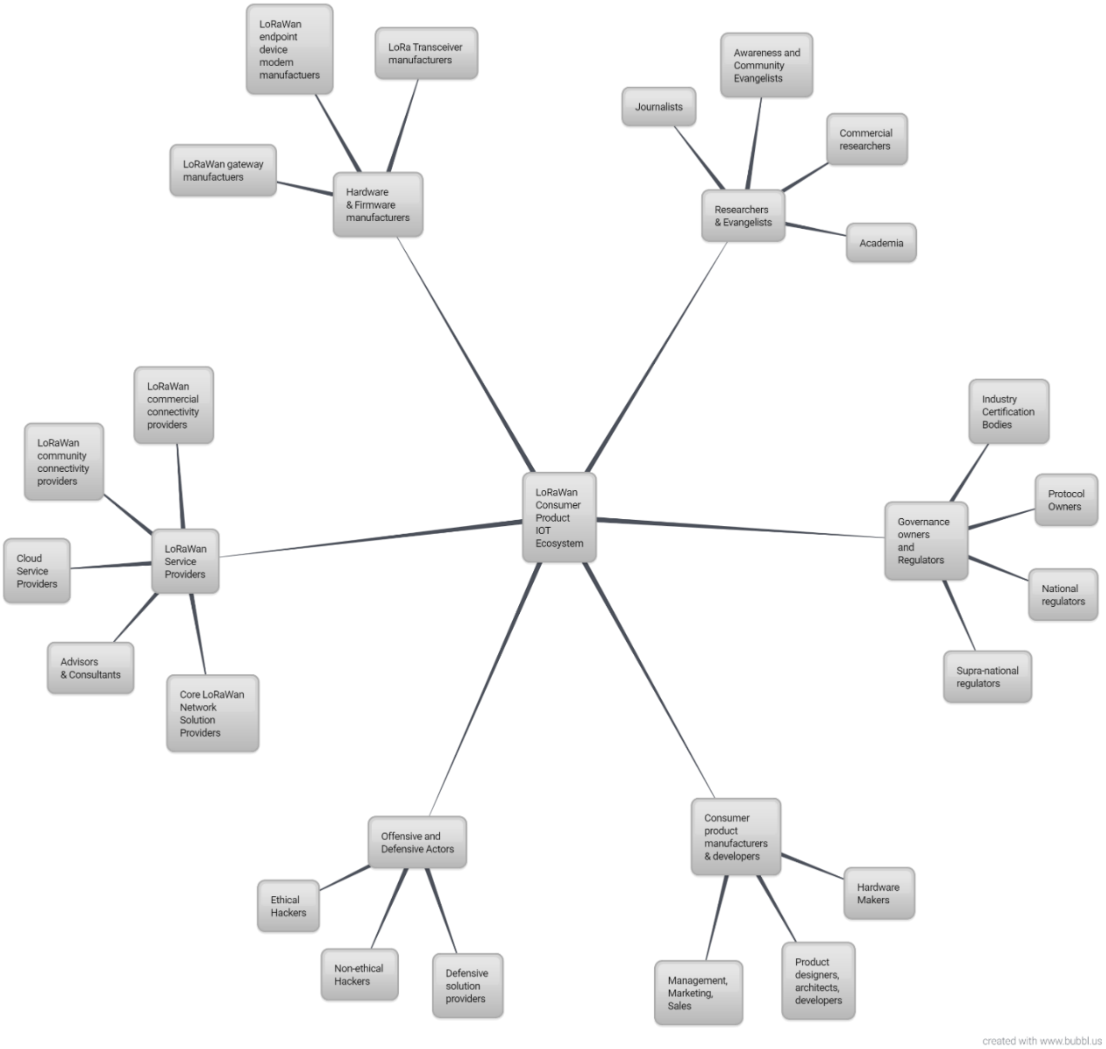
LoRaWan endpoint device modem manufactuers
LoRa Transceiver manufacturers
LoRaWan gateway manufactuers
Hardware & Firmware manufacturers
Journalists
Awareness and Community Evangelists
Commercial researchers
Researchers & Evangelists
Academia
LoRaWan commercial connectivity providers
LoRaWan community connectivity providers
LoRaWan Service Providers
Cloud Service Providers
Advisors & Consultants
Core LoRaWan Network Solution Providers
LoRaWan Consumer Product IOT Ecosystem
Industry Certification Bodies
Protocol Owners
Governance owners and Regulators
National regulators
Supra-national regulators
Offensive and Defensive Actors
Ethical Hackers
Non-ethical Hackers
Defensive solution providers
Consumer product manufacturers & developers
Hardware Makers
Management, Marketing, Sales
Product designers, architects, developers
created with www.bubbl.us

Figure 6: Specific LoRaWan Ecosystem Stakeholders used as a model for selecting experts and scheduling interviews.

3.2.4 Interview Guide

In order to conduct quality interviews and collect data that can later be analyzed and used to draw good conclusions an interview guide was created, refer to Table 1. The guide serves as an indication of which questions were asked during the interviews to which stakeholder groups. Not all questions are applicable to each stakeholder group as visible from the guide. Questions are further split into a small number of areas in line with the main research question. These questions were not asked literally in many cases, nor in the order as listed in the guide. The guide serves as a list of areas that were discussed with experts; actual questions will be tailored based on the background and interest of each individual interviewee, and in many cases follow-up questions were asked that are not listed in the guide.

All questions listed in the guide should be understood and interpreted in the context of LoRaWan-connected consumer products.

Table 1: Interview Guide

Question	Hardware / Firmware manufacturers	LoRaWan Service Providers	Offensive / Defensive Actors	Product teams	Governance & Regulators	Researchers & Evangelists	Consumers
GENERAL INTRODUCTION AND SECURITY							
What do you imagine when I say security for IOT consumer products?	X	X	X	X	X	X	X
As an actor in the ecosystem around LoRaWan, what do you expect from the system when it comes to security?	X	X	X	X	X	X	X
What is your biggest security concern?	X	X	X	X	X	X	X
RESPONSIBILITY							
Who should in your opinion be responsible that the system is secure? (interviewer explains the mind map of the most important the actors)	X	X	X	X	X	X	X
Whose task is it to prevent the consumer from the threats and vulnerabilities? Your task?	X	X	X	X	X	X	X
What role do you see for yourself in the quest to make the ecosystem secure?	X	X	X	X	X	X	X
What role do you see for regulators in making the ecosystem secure?	X	X	X	X	X	X	X
What role do you see for end users in making the ecosystem secure?	X	X	X	X	X	X	X
What role do you expect from academia?	X	X	X	X	X	X	
CONNECTION BETWEEN ACADEMIA AND INDUSTRY							
Should academic research be concerned with what's happening in the industry?						X	
How can PPP (public-private-partnerships) play a role?		X		X	X	X	
Who should be the recipient of the scientific papers and evangelic talks, which actors should read them and act on them?						X	
What is in your opinion the root cause of the difference between the industry view and academia view?	X	X	X	X	X	X	
How should the industry frameworks reflect the results of academic research?						X	
IOT FRAMEWORKS							
What do you expect from security frameworks? Do you use them / would you use them, and why (not)?	X	X	X	X	X	X	
If you want to learn about the security of the ecosystem, where would you go, what would you do?	X	X	X	X	X	X	X
How did you take IOT frameworks, or known vulnerabilities into account when designing and implementing the consumer product? What would be the ideal process?				X			
IMPACT OF KNOWN VULNERABILITIES AND THREATS							
Do you understand the identified vulnerabilities and threats? Do you think you should understand?	X	X	X	X	X	X	X
Based on the research, how did your view of the impact on citizens change?	X	X	X	X	X	X	X
What would be the vulnerabilities you would start exploiting?			X				
How would you monetize these vulnerabilities?			X				
Do you find the identified vulnerabilities interesting to exploit and gain value from?			X				
What exploits have you encountered related to the identified vulnerabilities?		X	X	X			

Which vulnerabilities and threats do you see important enough to start mitigating? Which ones are important enough to be on your agenda?	X	X	X	X	X	X	
LOOKING BACKWARD AND GOING FORWARD							
How should we address the security vs. usability problem for LoRaWan? Who should make the decision?		X		X	X		
What would you recommend consumers to do? Should they do something?	X	X	X	X	X	X	
Who should perform the risk assessment on behalf of end users/citizens when using consumer IOT products? Should they know what the risks are and how to mitigate them?				X	X		
How should be the security requirements for the final product defined, to ensure that the product meets obligations towards making the ecosystem secure?				X	X		
Where do you see currently the biggest gap in addressing the security question? Who is lagging the most behind?	X	X	X	X	X	X	
How would you protect the consumer against these vulnerabilities?			X				

3.2.5 Stakeholder Interviews

Stakeholders were selected for the interviews based on the stakeholder model for IOT LoRaWan consumer product ecosystem. Interviews were scheduled based on availability with the goal of covering variety of opinions from different stakeholder groups. Each interview took between 30 and 60 minutes, and loosely followed the interview guide. Interviews were planned upfront and took place in a private setting. Each participant was informed about the purpose of the research, and gave an informed consent with participation and the process either via email or verbally before the interview. Most interviews were tape recorded and typed into a word document. One interview was conducted via email. One interview was conducted without tape recorder with notes being captured after the interview.

Table 2Table 3 shows the list of experts who participated in the interviews, together with their profession and short explanation why their expertise is relevant for the research. In order to protect the privacy of the experts, they are represented by a unique Code Name. This code name is used to further refer to the interviewee throughout this study.

Table 2: List of experts who participated in the interviews

Code Name	Profession & Relevant expertise for the research
A	Member of D66 Leiden, Cyber Security Consultant. In both of those roles combines technology and politics.
B	Security analyst for a large bank, working in Security Operating Center
C	Management Consultant, works for a network provider that owns a nationwide LoRaWan network, has a publication in the area of LoRaWan security
D	University Professor and Researcher in the area of networks. Implemented a LoRaWan pilot for a governmental organization.
E	Student with interest in security of LPWAN ZigBee networks.
F	Cyber Security Consultant, with passion for IOT (e.g. built his own IOT network at home).
G	Experienced management consultant with background in IT and Cyber Security
H	Specialist with background in security and engineering, DIY IOT engineer
I	IOT consumer device manufacturer, LoRaWan is the network protocol used in the manufactured devices
J	Security Analyst for a large bank with background in Security Risk Assessments, and Operational Security.
K	Management Consultant with focus on strategic thinking in IT and Technology.
L	Two ethical hackers for a consulting form purely specialized in Cyber Security
M	Management Consultant with focus on strategic thinking in IT and Technology.

3.2.6 Coding Manual

Table 3 lists the coding manual used for coding the data collected from expert interviews.

Table 3: Coding Manual

CATEGORY	CODES
General Topics	1) IOT Security Definition 2) Business vs. Security in LoRaWan 3) Business vs. Security in Product 4) Business vs. Security in Network Provider
Responsibilities	5) Consumer Responsibilities 6) Manufacturer Responsibilities 7) Network Operator Responsibilities 8) Academia Responsibilities 9) Awareness People Responsibilities 10) Consultants & Experts 11) LoRa Alliance Responsibilities
Threats, Vulnerabilities, Controls	12) General threats, vulnerabilities, controls 13) Design of threats, vulnerabilities, controls 14) Use Case for LoRaWan
Attack	15) Attack vectors & actors 16) Impact of attack 17) Defense mechanisms
Ideas, Inspiration, Forward Looking	18) User Friendliness 19) How to do it right 20) Regulation 21) Certification 22) Cooperation
Problem, Concern, Challenge	23) Knowledge of product teams 24) Privacy 25) Reasonable Security Profession 26) Information Asymmetry 27) Externality 28) Problems with the LoRaWan standard 29) Lack of Awareness 30) Insufficient incentives 31) Supply Chain & Security 32) Consumer is the weakest link
Other	33) ZigBee vs. LoRaWan 34) Frameworks 35) Drawing Parallel 36) The bigger picture

4 Phase 1: Desktop research - Security Risk Assessment of LoRaWan connected Consumer Products

4.1 Research question for desktop research

In this chapter we ask the following question: what are the known cyber security threats, vulnerabilities and recommended counter-measures?

As a reminder, the use case considered in the thesis is a consumer-grade IOT devices connected to the network with LoRaWan protocol version 1.0.2 class A. We are only considering those cyber security threats, vulnerabilities, and counter-measures that are related to the LoRaWan network communication.

The methodology used to answer the question is explained in Chapter 3.

4.2 Applicable check-lists for threats and measures

The first step of identifying known cyber security threats and mitigating controls or counter-measures was to gather list of applicable existing guidelines. We started with the list of Security and Privacy guidelines collected by Bruce Schneier [31]. For each guideline, we identified whether it is suitable for the LoRaWan/ioTracker use case or not. This resulted in 11 guidelines that were further considered in the research. Table 4 summarizes the results.

Table 4: Existing IOT check-lists (guidelines and frameworks) considered as input to the research

ID	Check-list Name	Publishing Organization	Release Date	Release Version	Suitable for this research
F01	Internet of Things (IoT) Security and Privacy Recommendations [32]	Broad Internet Technical Advisory Group	Nov-2016	N/A	Yes
F02	IoT Security Guidance [33]	OWASP	24 November 2016	24-11-2017	Yes
F03	Strategic Principles for Security the Internet of Things (IOT) [34]	U.S. Department of Homeland Security	15 November 2016	Version 1.0	Yes
F04	Technical report Security [35]	OneM2M	30 August 2016	TR-0008-V2.0.0	Yes
F05	Technical report Security Solutions [36]	OneM2M	30 August 2016	TS-0003-V2.4.1	No
F06	IoT Security Guidelines Overview Document [37]	GSM Association	08 February 2016	Version 1.0	No
F07	IoT Security Guidelines for Service Ecosystems [38]	GSM Association	08 February 2016	Version 1.0	Yes
F08	IoT Security Guidelines for Endpoint Ecosystems [39]	GSM Association	08 February 2016	Version 1.0	Yes
F09	IoT Security Guidelines for Network Operators [40]	GSM Association	08 February 2016	Version 1.0	Yes
F10	Establishing Principles for Internet of Things Security [41]	Internet of Things Security Foundation	N/A	N/A	Yes
F11	IOT Design Manifesto [42]	Afdeling Buitengewone Zaken, Beyond.io, FROLIC Studio, The Incredible Machine	May 2016	Version 1.0	No

F12	New York City Guidelines for the Internet of Things [43]	City of New York	N/A	01-10-2017	No
F13	IoT Security Compliance Framework [44]	IoT Security Foundation	2016	Release 1.0	Yes
F14	Future-proofing the Connected World [45]	Cloud Security Alliance, IoT Working Group	2016	N/A	Yes
F15	IoT Security & Privacy Trust Framework [46]	Online Trust Alliance	14 October 2017	Version 2.5	Yes
F16	Five Star Automotive Cyber Safety Framework [47]	I Am The Cavalry	February 2015	N/A	No
F17	Hippocratic Oath for Connected Medical Devices [48]	I Am The Cavalry	January 2016	N/A	No
F18	Industrial Internet of Things Volume G4: Security Framework [49]	Industrial Internet Consortium Security Working Group	26 September 2016	IIC:PUB:G4:V1.0:PB:20160926	No

Three guidelines specific to a certain industry with large differences with consumer products were out-scoped. Namely guideline F16 is specific to the automotive industry, guideline F17 is specific to medical device industry, and guideline F18 is specific to industrial IOT products (e.g. SCADA devices). Guideline F12 is specific to the governments, non-for-profits and companies operating in the New York City and was thus also not considered. Guideline F11 was not specific to cyber security, and in fact was only a very generic leaflet. Guideline F05 was a meta-document explaining how to read guidelines F06-F08 and did not contain any specific risks or mitigating recommendations.

The guideline closes to the use case of this research is F15, which states that it is specifically focusing on IOT Consumer Products.

No specific guideline was identified that discusses security of LoRaWan connected IOT devices.

Most of the guidelines focused on controls and countermeasures. Threats were discussed only in two documents, namely F01 and F04. The remaining documents are focused on recommended mitigations.

4.3 Threats

Using the defined methodology, the following 6 threats known by IOT Frameworks were identified that are supposedly relevant to the studied use case. Unlike a vulnerability, a threat is in general more high level and less specific to the LoRaWan technology.

Each of the identified threat is briefly explained. It is not the goal of the thesis to conduct an in-depth research and discussion of the identified threats, they are generally well known or discussed elsewhere.

The threat actors are the same for all of the identified threats. We can group them into three categories: (a) actors on the side of the network operator; (b) persons with a radio able to intercept the LoRaWan signal. This can be achieved with a low cost of the shelf product. (c) actors, e.g. malicious software or hacker exploiting one of the communicating endpoints (e.g. the IOT endpoint, or the gateway) which have access to network.

4.3.1 Eavesdropping of messages

A threat exists that the content of a message transmitted over LoRaWan or a part thereof is intercepted during transfer by a third party that is not an authorized recipient of the message (e.g. a threat agent intercepting the wireless communication). This is an attack against confidentiality of the communication.

This could either be caused by unencrypted communication whereby messages are sent in plain text and readable to anyone who intercepts them; or alternatively by a weak or vulnerable encryption protocol that exposes part of the communication. The threat includes interception of encryption keys that are used to encrypt the message.

As a result, this leads to a leakage of sensitive user information, which can include privacy related data.

4.3.2 Alteration of Messages

The threat describes a situation where part of the LoRaWan-transmitted message is altered without the communicating parties (i.e. the IOT consumer device and the IOT gateway) noticing it. By altering part of the message, the attacker may deceive or fraud the stakeholders. This is an attack against integrity of the communication.

4.3.3 Replay of Messages

A threat that the LoRaWan transmitted message will be re-sent by an unauthorized party and that the recipient (i.e. the IOT device or gateway) will consider the duplicate message as valid. Repeating part or whole message between components can deceive or fraud the stakeholders.

4.3.4 Unauthenticated or Unauthorized Communication

The threat describes a scenario where the IOT consumer device or gateway allows a network connection from an unauthenticated or unauthorized device (i.e. a gateway accepting messages from a rogue IOT device or an IOT device accepting messages from a rogue LoRaWan gateway).

The network is responsible for establishing trust between devices and should assume that by default devices that have not been authenticated are untrusted. A complication is that many IOT endpoints are located in an open environment, where physical security cannot be guaranteed.

An attacker could exploit the threat and force a device to reveal information about its owner, or change the integrity of the software installed on the device.

4.3.5 Lack of Network Isolation

The threat describes the situation where devices are not isolated from each other on the network and cannot defend against a malicious actor already active in the network.

The threat is less relevant in the context of the nation-wide deployment of a LoRaWan network, but will become more applicable in situations where private LoRaWan solutions are available to home owners and consumers who wish to build a private local area network.

The threat could increase a risk that malware spreads from one device to another across the network.

4.3.6 Loss of Connectivity to the Network

Connectivity to the device may be interrupted, due to a radio interference, or a loss of service from the network provider e.g. due to a human error, or natural disaster.

Depending on the purpose of the communication devices, this could lead to financial losses for the consumer, loss of comfort, or in some cases safety risks.

4.4 Mitigating Measures (part 1: industry check-lists)

The research revealed the following 8 categories of specific technical countermeasures that the technology should offer in order to mitigate the existing threats described in the previous section. In this section, each countermeasure is briefly explained. As mentioned before, due to the low power and simple nature of the endpoints in IOT, it is expected that as many countermeasures as possible are offered out of the box by the network layer. For that reason, we discuss each countermeasure in the context of how well it is supported by the LoRaWan specification version 1.0.2 class A.

4.4.1 Encryption of the Communication

Requirement: data in transit on the network communication is encrypted by default using current generally accepted security standards and the communicating devices and applications must make use of the encrypted communication.

LoRaWan situation: Countermeasure is implemented.

LoRaWan communication is in all situations encrypted using AES128 in Counter Mode. However, unlike in SSL or other cryptographic applications, the devices and associated applications have no possibility to influence which cryptographic protocols will be used.

4.4.2 Firewall

Requirement: Implement a firewall to monitor and control incoming and outgoing traffic.

LoRaWan situation: Countermeasure is not implemented.

The protocol does not offer any possibilities to limit on the endpoint what type of traffic will be permitted, or blocked.

4.4.3 Replay Protection Countermeasure

Requirement: Detect if all or part of the transmitted message is an unauthorized repeat of an earlier message or part of a message.

LoRaWan situation: Countermeasure is implemented.

General protections against replay attacks are (a) tagging messages with session IDs and component numbers; (b) one-time passwords that expire after each use, or after a very short amount of time; (c) nonce - arbitrary numbers that can be used only once and add randomness to each transmitted message; (d) Timestamps which ensures that messages are only received at the moment they are sent, and that later replayed messages are disregarded.

4.4.4 Protection against Unauthorized Connections

Requirement: The product network protects the device against unauthorized connections at all levels of the protocol.

LoRaWan situation: Countermeasure is implemented

LoRaWan 1.0.2 class A limits connectivity to the end devices only to a short timeframe after the end device started communicating. Messages are encrypted, and protected with message integrity code, therefore unauthorized connections are unlikely.

4.4.5 Secure Key Management

Requirement: store all communication keys securely.

LoRaWan situation: Countermeasure is not implemented.

Two different methods exist for distributing the encryption keys. One is called OTAA (over the air activation), where the device is identified into the network and security keys are negotiated and stored on the device. How the keys are stored is not discussed in the LoRaWan protocol. The second method is called ABP (activation by personalization). In this situation the security keys are hardcoded into the device before the device joins the network.

4.4.6 Network Resilience

Requirement: Where there is a loss of communications it shall not compromise the integrity of the endpoint device.

LoRaWan situation: Countermeasure is implemented.

The protocol does not specifically describe or address this counter-measure explicitly. In case of LoRaWan 1.0.2 connected endpoint devices, two scenarios are possible: (a) the endpoint needs to be able to recover and maintain integrity in the case that the network stopped operating (e.g. due to a loss of service on the LoRaWan gateways). This should be achieved by re-activation and re-connecting to the network; and (b) the endpoint needs to be able to remain integrity in case that the LoRa antenna on the network itself stopped working. In that situation the device will no longer be connected to the network and thus the threat is irrelevant.

4.4.7 Identification on the Network

Requirement: Devices should identify themselves to a network using a secure identifier.

LoRaWan situation: Countermeasure is implemented.

LoRaWan knows a unique identifier for devices and applications: DevEUI - a global identifier that uniquely identifies the end device, and AppEUI - a global identifier that uniquely identifies the application.

4.5 Mitigating Measures (part 2: academic check-lists)

This section looks at the LoRaWan specific counter-measures that are known in the academic world.

Tanenbaum & Wetherall state that network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, nonrepudiation, and integrity control [50].

The industries take a broader view and define that "network security encompasses the structures, transmission methods, transport formats, and security measures used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media" [51].

A targeted research goes even further. A security comparison of LPWAN technology considers the following characteristics as relevant for assessing security of a the network protocol: (a) existence of global unique identifiers, (b) authentication of device, subscriber and network, (c) privacy-preserving identity protection, (d) data confidentiality, (e) end-to-middle security, (f) forward secrecy, (g) integrity protection, (h) replay attack protection, (i) reliability of delivery, (j) existence of access classes for critical infrastructures, (k) updatability of device, (l) updatability of keys and algorithms, (m) network monitoring and filtering, (n) key provisioning, (o) ability to negotiate cryptographic algorithms, (p) resistance to class breaks, (q) requirement for mandatory device certification, and (r) the ability to layer IP protocol over the LPWAN protocol [52].

This chapter provides an evaluation of the LoRaWan performance against this benchmark. Each requirement from the benchmark is very briefly introduced. Consequently, a discussion follows about how well the requirement is satisfied by the standard. In the discussion, knowledge of the protocol is expected. The terminology used is identical as defined in the LoRaWan standard.

4.5.1 Existence of Global Unique Identifiers

Requirement: Identification is the process where a device is identified in the population. This is a pre-requisite for a follow-up authentication. In order for the concept to work, the identification of each device must be unique.

LoRaWan situation: Countermeasure is implemented.

Each device contains a DevEUI, which uniquely identifies it globally in the IEEE EUI64 space. Before the activation step, a device also contains AppEUI, a global application ID that will identify the entity which will process the identification and key generation.

Devices that are destined for OTAA also contain a root AES key called AppKey which should be specific for the device. However, the protocol does not discuss how that is ensured, and it remains an open question. This key is used during the OTAA process.

Once the device is activated (OTAA or ABP), it is provisioned with the following identifier: a 32-bit end-device address (DevAddr) which identifies the device uniquely within the network within which it was activated. Part of the DevAddr is reserved to uniquely identify the network itself.

4.5.2 Authentication of device, subscriber and network

Requirement: The endpoints should uniquely authenticate on the network before data messages are exchanged.

LoRaWan situation: Countermeasure is implemented.

The provisioned keys authenticate the endpoint device. Specifically, NwSKey authenticates the device itself, and AppSKey authenticates the application or subscriber. Before the activation step, the root AppKey authenticates both.

4.5.3 Privacy-Preserving Identity Protection

Requirement: Minimize the use of a static global identifier which could be used to intercept and correlate data about a single individual over time.

LoRaWan situation: Countermeasure is not implemented.

Upon activation, each device is provided with a unique and static DevAddr. DevAddr only changes upon re-activation and it is not mandated by the standard that the device address should change in that situation. In conclusion, LoRaWan provides only a very limited privacy-preserving identity function.

4.5.4 Data Confidentiality

Requirement: All data communication and sensitive control information is encrypted using a strong cryptographic algorithm. It is not feasible for the attacker to derive any information about the original message been transmitted in case the communication is intercepted.

LoRaWan situation: Countermeasure is implemented.

The data frame payload of the LoRaWan communication is by default automatically encrypted using a symmetric encryption, AES, with a key length of 128 bits as described in IEEE 802.15.4/2006 Annex B. Two various encryption session keys are used. An application session key (AppSKey) for encrypting the payload field of application specific data frames. The second key is a network session key (NwkSKey) for encrypting payload of network administration messages.

The reason for choosing a symmetric algorithm is its lower computational complexity. Many endpoints will be low power and simple devices that would be overloaded with an asymmetric encryption algorithm.

The following communication is not encrypted: communication other than the frame payload (MAC header, frame header, frame port, MIC), Join-Request messages.

4.5.5 End-to-Middle Security

Requirement: End-to-Middle security describes security context between the endpoint devices and the LoRaWan network server, dealing with a situation where intermediaries (gateways) are less trusted. The concept applies both to confidentiality as well as integrity of the communication.

LoRaWan situation: Countermeasure is implemented.

Due to the simplicity of the LoRaWan architecture, end-to-middle security is easily provided using the AppSKey which provides confidentiality of the communication between the endpoint device and the server.

4.5.6 Forward Secrecy

Requirement: Forward secrecy is a property of the communication protocol, where compromise of long-term keys does not lead to a compromise of past session keys. The property does not guarantee security of the protocol after the key is compromised. The available encryption algorithms that provide forward secrecy are unfortunately very resource intensive and not suitable for low power devices.

LoRaWan situation: Countermeasure is not implemented.

Forward secrecy is not guaranteed. If an endpoint device is compromised, an attacker can calculate with minimum effort the session keys. For that he would need to know AppNonce and DevNonce, which are easy to brute force parameters.

4.5.7 Integrity Protection

Requirement: The recipient of the message must be able to detect unauthorized changes by a malicious actor. Since the data payload is often stored on another layer in the protocol stack than the control information (e.g. port number), the network standard must consider separately integrity of data and integrity of control information.

LoRaWan situation: Countermeasure is implemented.

Message integrity code (MIC) is calculated over the following fields of the message: MAC header, Frame Header, frame port, frame payload. The encryption primitive used is also AES128 and the MIC calculation follows RFC4493. The key used is NwkSKey. This provides integrity of both the message and the control information.

4.5.8 Replay Attack Protection

Requirement: Communication recorded by an attacker and re-sent (replayed) at a later moment is not accepted by the receiving party as a legitimate.

LoRaWan situation: Countermeasure is implemented.

We will consider two scenarios separately: the over-the-air activation (OTAA) step, and regular communication.

During the OTAA, which consists of join-request and join-response handshake, join-request messages contains a random value (called DevNonce). For each communicating endpoint device, the network server keeps track of previous DevNonce values and will disregard any duplicate communication. The join-request is protected with a message integrity code to prevent attackers sending an arbitrary join-request on behalf of an endpoint.

For data communication, the network provides replay attack protection using uplink and downlink frame counters, which are kept up-to-date both on the server side and endpoint device side.

4.5.9 Reliability of Delivery

Requirement: The network should detect if a message is not delivered to the intended recipient, e.g. because selective messages have been blocked.

LoRaWan situation: Countermeasure is not implemented.

LoRaWan has limited acknowledgement capabilities, which may draw it unsuitable for certain use cases.

4.5.10 Existence of Access Classes for Critical Infrastructures

Requirement: The concept of quality of service is known to the industry for long time. In situations where certain type of traffic needs to be prioritized over other, the network should have capabilities to guarantee that. This could mean that for example critical infrastructure traffic is prioritized over consumer-grade connections.

LoRaWan situation: Countermeasure is not implemented.

The concept is not introduced in any version of the LoRaWan protocol.

4.5.11 Updatability of Device

Requirement: The ability to update a device is not a network issue per-se. However, the network design and architecture should make it feasible for the device manufacturers to manage vulnerabilities in the firmware and operating system, as well as application owners to provide updates to the software running on the endpoints. It is a known fact that vulnerabilities are discovered on a daily basis, and no system will ever be vulnerability free. Having a possibility to patch vulnerabilities remotely is a key requirement for a secure ecosystem.

LoRaWan situation: Countermeasure is not implemented.

The LoRaWan specification currently does not allow for any patching over the air.

4.5.12 Updatability of Keys and Algorithms

Requirement: The network protocol should provide mechanism for renewal or rotation of long-term root keys stored in the endpoint devices. It is a known fact that with the lifetime of a key increases the probability that the environment which is protected by the key will be compromised. Certain regulations may mandate that keys are regularly rotated.

LoRaWan situation: Countermeasure is not implemented.

There is no mechanism in place to replace the AppKey in the device in case of OTA activation and NwkSKey, AppSKey in case of ABP other than replacing the entire endpoint device.

4.5.13 Network Monitoring and Filtering

Requirement: The standard should discuss requirements for network monitoring, both for unencrypted metadata, and deep packet inspection for encrypted data. Having a possibility to firewall the communication, monitor traffic and detect malicious behavior on the network may be necessary especially in the ecosystem of low power devices that do not have enough capacity to ensure this capability alone.

LoRaWan situation: Countermeasure is not implemented.

Network monitoring is not considered in the standard. Network operators can implement monitoring as an additional service on top of the standard requirements.

4.5.14 Key Provisioning

Requirement summary: the protocol should consider mandating how cryptographic keys are provisioned to the endpoint devices, and how they are stored. Although the low power nature of many endpoint devices might not allow it, the standard should at least discuss the option of using a secure element in the device and HSM on the service provider side.

LoRaWan situation: Countermeasure is partially implemented.

To participate in LoRaWan network each communicating endpoint device must be activated. Key generation and distribution is part of this step. Once done, two session keys are provisioned to the device: a network session key (NwkSKey) and an application session key (AppSKey).

The protocol recognizes two possibilities: over-the-air activation (OTAA) and activation by personalization (ABP).

Devices that are destined for OTAA contain a root AES key called AppKey which is also known by the application server. The application server derives the NwkSKey and AppSKey using a simple key generation procedure and shares it with the endpoint device encrypted using the AppKey.

During ABP, both NwkSKey and AppSKey is hardcoded into the device using an out-of-bound channel, which is out of scope for the LoRaWan protocol.

No matter if the device will activate using OTAA or ABP, there are always keys stored in the device by the manufacturer (NwkSKey, AppSKey in case of ABP, and AppKey in case of OTAA). No requirements are described in the standard with regards to the key management and security of the keys. How keys are stored and protected is outside the scope of the protocol and remains a challenge to be solved by the device and application manufacturers. It is also out of the scope for the LoRaWan protocol how the root AES key is distributed, and how keys are decommissioned, rotated, or invalidated.

Furthermore, the LoRaWan protocol expects for the following steps a random number input: random DevNonce needs to be calculated by the endpoint for join-request messages during the OTAA process. Similarly, the server calculates a random AppNonce during the join-response. Moreover, in some cases delays between transmissions of two messages should be randomized by the communicating devices.

Calculating strong pseudo-random generator is a known and difficult process, and unfortunately the LoRaWan specification only gives a marginal recommendation about how that should be done. The network does not provide any services in that respect.

4.5.15 Ability to Negotiate Cryptographic Algorithms

Requirement summary: The standard should anticipate on changes in trust for different cryptographic protocols. On yearly basis, vulnerabilities and weaknesses in known cryptographic protocols are discovered, and known encryption becomes obsolete or less suitable for certain use cases.

LoRaWan situation: Countermeasure is not implemented.

The LoRaWan standard has no mechanism in place for the endpoint device to specify which algorithm should be used, giving deployments the choice to select a stronger cryptographic primitive for certain use cases. The only option is the use of AES128 both for encryption and signing.

4.5.16 Resistance to Class Breaks

Requirement summary: In order to prevent class breaks network protocols should be constructed in such a way that endpoint devices cannot share the same encryption keys. This prevents a situation where if one key is compromised, other devices are at risk. The requirement is especially important for consumer products, where it is expected that devices from one manufacturer are identical and security is typically not a priority for the owner.

LoRaWan situation: Countermeasure is implemented.

The single most important key for LoRaWan deployments is the root key of the endpoint (AppKey). The standard says that AppKey should be unique for each device. Yet the standard does not specify how the requirement can be met, or whether the network operator should act if this is not the case. In theory, it is possible that a device manufacturer will issue all devices with the same AppKey leaving the product vulnerable to class breaks. The LoRaWan network server has access to AppKeys for devices that are provisioned to the network, and could build alerts for a situation when multiple devices have the same AppKey.

4.5.17 Requirement for Mandatory Device Certification

Requirement summary: Network operators should be issuing access (e.g. encryption keys) only to those devices for which the manufacturer has gone through a certification process. Certification ensures that the devices operate in line with regulation for devices transmitting radio signals.

LoRaWan situation: Countermeasure not implemented.

The requirement could be optionally enforced by the network operator. The LoRa Alliance offers a certification process for device manufacturers. However, as far as known to the author, there is no network operator who follows that route. LoRaWan is the only widely known LPWAN protocol that does not enforce certification.

4.5.18 The Ability to Layer IP Protocol Over the LPWAN Protocol

Requirement summary: layering security protocols is beneficial to enable interoperability, internetworking and reuse of known protocols. Ability to for LPWAN protocol to operate together with IP protocol brings certain advantages, and it is recommended that the protocol provides the option.

LoRaWan situation: Countermeasure is not implemented.

LoRaWan is not built out of the box to be used together with IP protocol. The data frame layer is directly usable for application specific data and no further protocols are necessary. This is by many considered a competitive advantage rather than a weakness of the standard.

4.6 Threat Actors

In the following sections we will study vulnerabilities in the LoRaWan protocol and its possible implementations. A common approach to study and assess vulnerabilities in certain environment is to adopt the role of an attacker. Therefore, before we dive into description of the specific vulnerabilities, we will shortly discuss the typical attackers that will be considered.

Building a complete framework around the existing threat actors is beyond the scope of this thesis. We will distinguish two types of attackers: low-profile and high-profile attackers.

By a low-profile attacker, we mean someone with malicious intentions but without any additional access other than what is publicly available. Such an attacker will be able to gain a detailed knowledge of the LoRa and LoRaWan protocol, be able to purchase consumer-grade endpoint devices, subscribe to the available public LoRaWan networks or even establish his own rogue network using commercially available of the shelf hardware. He will be able to intercept data in the wireless radio band, and send a legitimate or malicious signal. This profile will represent a typical low-end attacker, either lonely wolf or someone acting in a small organized group. Providing a suitable knowledge, it should be possible to assume the role of this type of attacker over-night, without significant financial investment, or access to people that normal person would not have. His motives will most likely be either financial, trying to either monetize his attacks, or a pure curiosity, trying to see what it is technologically possible and how far one can reach, such as script kiddies.

By a high-profile attacker, we will consider someone beyond what a regular citizen can achieve in a short amount of time. It will be either someone with insider knowledge to the IOT LoRaWan ecosystem, e.g. the network operating company, backend infrastructure, or with access to people that can significantly ease his attack. High-profile attackers will often be either knowledgeable insiders, organized crime gangs or even nation states with sufficient financial and time resources. We will also consider governmental bodies as part of this group. Although in many cases their intensions are not typically with intrinsic malicious intentions, some of the actions can be perceived by citizens as such. High profile attackers have the ability to for example gain control of a whole LoRa network, or attack servers that are not directly connected to the IOT world or internet.

There might be cases on the border of both groups such as hacktivists where one can argue for both options, and although the categorization is very sophisticated, it is sufficient for the case of studying vulnerabilities in consumer-grade IOT devices connected to LoRaWan networks.

4.7 Vulnerabilities in the design of the protocol

This section describes vulnerabilities and weaknesses in the design of the LoRaWan protocol.

In the very basic form, computer network consists of hosts and links. In case of LoRaWan we consider, gateway and endpoint IOT devices to be the hosts, and the connection between them to be the link.

This research focuses mainly on security of the link, and the host that represents the IOT endpoint device. We will also briefly consider those vulnerabilities in the LoRaWan gateway and on the server-side, only to the degree where they are directly linked to a weakness in the LoRaWan standard, or its implementation.

In this section we focus on vulnerabilities and weaknesses in the design of the LoRaWan protocol. For simplicity, we will call both weaknesses and vulnerabilities just vulnerabilities.

The research is done based on the latest final version of the protocol at the time the research started. That is version 1.0.2 published in July 2016 [53]. A version 1.1 of the protocol is currently in a draft phase, and has not yet been published. It is also possible that devices and networks implement older versions, e.g. 1.0. None of these were considered in this research.

4.7.1 Insecure Device Activation Option

The LoRaWan protocol design recognizes two ways in which devices could join the network and activate themselves: OTAA and ABP activation.

ABP is much less secure variant of the protocol due to the inability of the endpoint device to renegotiate session keys (AppSKey and NtwSKey) when deemed necessary. When using OTAA devices operating in exposed environments with high probability of physical compromise of the device can in extreme cases renegotiate session keys for each individual communication. Furthermore, OTAA allows devices to roam between networks and/or switch between different network providers. None of that is available in ABP. When keys are provisioned using ABP the device cannot switch between networks, and further, it is impossible to renegotiate new keys.

If keys are compromised, this exposes the rest of the communication between the device and the server for the lifetime of the endpoint device.

As a consequence, using LoRaWan in ABP mode is not considered secure and should be avoided as much as possible.

4.7.2 Vulnerabilities with OTAA and DevNonce

DevNonce is a random value which is generated by the endpoint device as part of the over-the-air activation procedure. The DevNonce history is remembered by the network server. Join-Request with DevNonce that has been used before is ignored. One function of this mechanism is thus to prevent replay attacks for OTAA.

This procedure as designed in the LoRaWan protocol has a number of vulnerabilities:

The first vulnerability in the design of the over the air activation procedure is that the Join-Request message which contains DevNonce is unencrypted (it is though signed) and thus unprotected against eavesdropping attack. The Join-Request message also includes AppEUI and DevEUI parameters, which although not by definition secret should not be unnecessarily exposed to anyone listening on the network. Reason for not utilizing encryption is that at that moment of the join request message, session encryption keys are not yet agreed and therefore encryption not possible. This vulnerability allows an attacker to listen on the network and gain insight into the behavior of the endpoint device and especially the DevNonce random number generation performance. Security of the random number generator implementation is often not very strong which further compounds the attack, refer to Section 4.8.5

The second weakness of the protocol is that the network server must decide how many past DevNonce variables it will remember. The number is not specified in the protocol and is subject to interpretation by the implementer. Any choice the implementer makes leads to vulnerabilities.

In case that the implementer decides to remember large amount of past DevNonce variables, this increases the chance that the endpoint device generates a value which has been remembered by the server, and thus the server will ignore the join request leading to DOS situations. If an endpoint device of a lifetime 10 years joins the network twice each day, this will lead to 7300 join-request attempts over the lifetime of the network. There are 2^16 possibilities of DevNonce variables. According to the birthday paradox, this gives approx. 11% chance that the device will send existing join request message towards the end of its lifetime. If on the other hand the implementer decides to remember a small amount of past DevNonce variables, this increases the chance of a successful replay attack.

Existing research has suggested two possible solutions to prevent the problem: (a) consider DevNonce to be a sequential number instead of randomly generated and adjust the protocol where necessary, and (b) increase the size of the DevNonce variable to reduce the probability of the collisions [54].

The replay protection is directly dependent on the strength of the above described mechanism.

4.7.3 Vulnerabilities in Design of Counters

Once an endpoint device is activated and connected to the network, it can start communicating messages towards the network server. In order to prevent replay attacks on these messages, the LoRaWan protocol defines uplink and downlink counters. After a data message is sent from the endpoint device to the network gateway, an uplink counter is incremented. In case a gateway receives a message which uses equal or lower value than the counter in the last communication, this message is not processed to prevent replay attacks.

The design of the counter functioning includes the following two vulnerabilities:

The first vulnerability is related to devices activated by person (ABP): The protocol states that once a device that is activated by person (ABP) is reset, the counter should also be reset to 0. For devices activated by person, encryption keys after reset remain the same, refer to Section 4.7.7. This means that the same encryption and integrity preserving keys will be used again with counter values that were used previously before the reset took place.

Therefore, if an attacker recorded a message from the endpoint device before the reset, this message can be replayed to the network server, and the message will be processed as valid. Furthermore, the counter on the server will be increased to the value in the malicious message, which may prevent messages from the legitimate device being processed, because the counter in those messages will be lower than on the server. That will lead to a denial of service until the legitimate endpoint device either resets the communication, or increases the counter to a value accepted by the server.

The likelihood of the attack will increase if an attacker (a) finds a way to identify devices which are activated by person, and (b) finds how he can enforce a reset of these devices. Counter values are not encrypted making it easier for the attacker to record and select the right message for the replay attack.

The second vulnerability is affecting both devices activated by person (ABP) and devices activated over the air (OTAA). The counter is designed as either 16bit or 32bit field, depending on the implementation. Once the maximum value of the counter is reached, the counter is rolled-over to zero. This means that an attacker who previously recorded messages between the device and server can successfully replay them. The probability of the attack is rather low since even 16bit counter is large enough to prevent frequent rollovers.

The attack has been practically demonstrated with success [55].

4.7.4 Decryption of messages for ABP devices

The encryption protocol used for devices activated on the network by person (ABP) includes a vulnerability that allows an attacker to decrypt the communication under certain circumstances.

Once an endpoint device is activated over the network, each communication towards the server is encrypted using AES128 in CTR mode. The message is XORed with a keystream generated using the Counter which is incremented with each new message. It is a known fact that for ciphers operating in counter mode, initiating vectors must not be reused with the same key for encrypting 2 different pieces of data.

However, there are situations where two different messages will be encrypted using the same keystream under the LoRaWan protocol. That will happen in case that the same Counter (initiating vector) was used to derive the keystream. That can happen in 2 cases as explained in Section 4.7.3. One possibility is in case that the device resets itself, which also resets the counter to 0. The other possibility is if the counter rolls-over itself as it reaches the maximum value.

It is a known vulnerability of ciphers in CTR mode that once two different messages are encrypted with the same keystream, the attacker can with some knowledge of one of the two messages decrypt the second message. This probability increases with the amount of messages that are encrypted with the same key. Assume for example that the attacker finds a way to reset the device after each communication and thus also reset the counter to 0, he will be able to force the endpoint to use the same keystream for each message sent, and thus with very high probability decrypt the whole communication.

4.7.5 Vulnerability to Radio Jamming

Radio jamming on the physical layer in general is a threat for wireless communication and inherent problem that every wireless signal needs to deal with [56], including the LoRaWan protocol [57]. The attack technique consists of an attacker generating powerful radio signal in the proximity of the senders or receivers which leads to disruption of legitimate traffic.

It has been shown by researchers that jamming LoRa signal can be achieved with of-the-shelf hardware commercially available in electronic stores for less than 30 EUR, namely an Arduino board with a strong LoRa antenna [58]. Approximately 99% of the LoRa transitions around the malicious actor can be affected by the attack. Targeted jamming individual senders is in theory also possible using a specific software which starts corrupting only the signal that is sent by specific LoRa antenna.

Good news is that there are ways to detect the attack. Communicating devices on free license bands are restricted in the amount of time that can be spent sending a signal and the minimum timeframe between two such sessions. In order for a LoRa jammer to be effective it would have to constantly occupy the spectrum, which is against the regulations and can lead to penalties.

Jamming attack can further be detected by a network operator, either by monitoring for sudden changes in communication patterns on the network or by monitoring for an abnormal behavior by an individual sender (e.g. too much activity on the network by individual sender).

4.7.6 Wormhole Attack

LoRaWan is by design be vulnerable to a so called Wormhole attack [58]. In this type of attack, a malicious actor first sniffs the communication between an endpoint IOT device and a LoRaWan gateway, then secondly jams the signal from spreading further, and thirdly replays the attack to another gateway at another location using another antenna. Because the original signal never reached the gateway, the uplink counter will not be incremented on the server, and the captured signal will remain valid and can be replayed as long as any signal from the original endpoint device is continued to be jammed. The vulnerability is compounded by the fact that there is no timestamp present in the design of the protocol making it possible for the attacker to replay the signal for indefinite period [59].

Depending on the use case of the device, this could have consequences, for example in case of the ioTracker, the service would identify the device to be located somewhere else that it in reality is.

A possible improvement of the LoRaWan protocol design would be to include a timestamp into the design of the protocol. Second improvement would be to introduce regulation for network operators to monitor for use cases that identify wormhole attacks. In case that a device suddenly changes its location or exhibits behavioral change with regards to its location that is not in line with the expectations, chances are high this was due to a wormhole attack.

4.7.7 Missing Process for Key Management

Implementation of key management in the LoRaWan protocol is missing. Under the current definition of the protocol, it is not possible to update the root keys in the endpoint device [60]. Keys can be leaked by various means, refer to Section 4.8.3. It is a known fact that root keys should be rotated regularly to reduce the likelihood of the compromise of the communication.

For devices that are activated over the air (OTAA), the root key is called AppKey. The AppKey is the most important secret used to generate session keys. While session can be generated multiple times based on the AppKey, the protocol does not provide any means for updating root device AppKey. For devices that are activated by person (ABP), session keys are directly hardcoded in the device. In this scenario, there is again no mechanism for updating the session keys. This is a much worse situation since these keys are directly used to encrypt and provide integrity of the communication.

This could lead to a situation where session keys are compromised and attackers can breach the confidentiality and integrity of the communication. There is nothing that can be done by service owners and manufacturers other than recalling the hardware endpoints and replacing the compromised keys. This is for large scale deployment very impractical, and in many cases impossible.

Multiple suggestions have been made to improve the (non)existing key distribution protocol.

One option is to distribute both static and session keys using Elliptic Curve Diffie Hellman (ECDH) in combination with Elliptic Curve Digital Signature Algorithm (ECDSA) protocol. These algorithms have been chosen for their low energy consumption and good security parameters. The suggestion would solve key distribution problem, because the generated keys could be used for which the current keys that cannot be updated are used [60].

Another proposed option is to use a reputation system to select trustworthy neighbors as helpers to calculate cryptographic functions, or even enhance the trust model with a probabilistic function based on Markov chains [61].

However, this has not yet been implemented and thus no mitigating control is available at the moment.

4.7.8 No Layer Independence for Key Generation in OTAA

The current NwkSKey and AppSKey generation under the OTA activation by network server does not respect the so-called network layer independence, whereby network keys and application keys are generated and owned by different parties.

In case of LoRaWan OTA activation, both NwkSKey and AppSKey keys are generated by the network server which introduces the risk that the server can act as a man-in-the-middle. Government can order the owner of the network infrastructure to intercept all communication in line with lawful interception laws, which exposes the entire network, similarly as exposed by Snowden files in the past. This scenario cannot be prevented unless the application owners implement additional end-to-end encryption on the application layer between the application server and the endpoint devices with secure key generation and distribution protocol.

Another consequence of the breach of layer independence is that network operators can duplicate devices owned by the end user, since they have all information that the endpoint device use to uniquely identify themselves on the network.

The vulnerability introduces a need for a trusted third party that could securely deploy a public key infrastructure on top of the existing architecture and generate and provision network keys to the application servers, and endpoint devices (through the network servers) during the LoRaWan activation procedure [62].

4.7.9 Gateway and DDOS

LoRaWan is organized as a star of stars, where gateways are in many cases a single point of failure. DDOS attack on one of the gateway would disconnect multiple endpoints from the network, namely those that signal reach to only that one gateway. Gateways are connected to the LoRaWan network and subject to jamming. Many gateways will also be connected to the internal IP-based network on the side of the operator, giving additional possibilities to a high-profile attacker.

A good solution to the problem is to cover the geographical area in such a way that each device has visibility over multiple gateways.

4.7.10 Message Integrity Code subject to Brute-force Attack

Each message in the LoRaWan communication is protected with a Message Integrity Code (MIC). This code prevents unauthorized modification of the message and can only be calculated by the communicating parties who have access to the session keys.

MIC is defined as a 4-byte field by the protocol, which is considered largely insecure by all today's cryptographic standards. 4 bytes equals 8 bits, which gives 2 to the power 8 possibilities (4 294 967 296) of various MICs. On average, an attacker will try half of that number to find the correct MIC code that signs a given message, that is 2 147 483 648 attempts.

That space of possible MIC values could be brute forced by a moderately powerful computer within milliseconds. Experiments have been done where average processing time for calculating the correct MIC based on the message is approx. 1500 milliseconds for an 8-core contemporary processor, and even less for in case a distributed system is used [63].

The attack has far reaching consequences. If an attacker can forge a signature of a message, that means he can also change encrypted message in transfer and generate a signature, which will make the message look legitimate. That does not yet give attackers a possibility to completely forge a plain text message, however, possibilities exist in that respect as well. That is discussed in the next section.

4.7.11 Bit-Flipping Attack

The LoRaWan protocol has been proven to be vulnerable to the Bit Flipping attack. Bit Flipping attack consists of attacker changing values in the encrypted message in such a way that he can control which bits will be changed in the original message [64]. By nature, it is always possible for an attacker to change bits in the encrypted message (since that message travels through untrusted environment), however, not all encryption algorithms suffer to the bit flipping attack, where the attacker can also control a position of the bits in the original text he changes.

Block cipher primitives are due to their design vulnerable to Bit Flipping attacks, including AES128 in Counter mode used in the LoRaWan protocol. A countermeasure has been proposed to introduce a two-phase shuffling method (shift phase and swap phase) to the encryption process that would prevent attackers from guessing position of bits in the unencrypted message [63].

The attack is compound by the fact that the message integrity code (MIC) is too simple and subject to brute-forcing, which allows attackers to perform the bit flipping attack without notice. Refer to previous section.

Furthermore, the network operator itself (e.g. the network server), if compromised can also perform the bit flipping attack, since it is in possession of the NwkSKey which can be used to recalculate the message integrity code after the bit-flipping.

4.8 Potential vulnerabilities introduced by poor implementation of the protocol

This section considers vulnerabilities that could arise from improper implementation or use of the LoRaWan protocol. This section especially considers those vulnerabilities where the protocol leaves room for implementation mistakes.

4.8.1 Possibilities for Insecure Key Generation

In both ABP and OTAA the way that session keys are derived and distributed could be implemented insecurely, which would increase the probability that they get compromised [60].

In case of ABP, session keys (NwkSKey, AppSKey) need to be generated and stored on the device before the device joins the network. The design of the protocol expects that the keys are generated randomly by an out-of-bound mechanism and hardcoded in the network. However, nothing stops the manufacturers to generate the keys based on a predictable pattern (e.g. the device ID, or the LoRa antenna hardware parameters). That would enable attackers to guess the keys and impersonate the communication.

In case of OTAA, the so called AppKey serves as a root key from which session keys (NwkSKey, AppSKey) are derived during the device activation. Similarly, as in the case of ABP, the device manufacturer could generate and distribute the AppKeys to the devices without sufficient randomization, which would increase the chance of compromise.

In extreme cases, keys that are distributed could be identical for all devices. This would allow an attacker to decrypt all communication once one device gets compromised.

4.8.2 Possibilities for further Attacks on Message Integrity

The protocol is designed to provide integrity of the messages by means of AES-based signatures. However, it is up to the implementation of the protocol to make sure that the signatures are validated. In case that the network servers do not validate the signature, it gives attackers possibility to change the cipher text message and thus adjust the plaintext message. To compound that, even if the network server validates the signatures, a high profile attacker could tamper with the integrity of the message after the signature is validated and removed by the network server, and message is forwarded to the application server for processing. The protocol does not define end-to-end integrity protection mechanism.

A specific variation of an attack on message integrity to which the protocol is further vulnerable is bit-flipping. Bit-flipping on the server side is possible due to the way that LoRaWan implements the encryption (XORing the plaintext with a keystream). If an attacker has knowledge of the basic structure of the plaintext message (e.g. the format), he can target specific bits in the plaintext to be changed by changing the same bits in the cipher text. The signature is no longer present during the transfer to the Application Server the server side, since it was removed by the Network Server.

There is no mechanism in the protocol that would encourage the receiver to validate the signature.

4.8.3 Possibilities for Insecure Key Storage

In the typical setup, each endpoint device contains a microcontroller unit (MCU) that performs the calculation, a LoRa chipset that ensures the communication, and a serial communication bus (either UART, or SPI) that connects the two. Currently, the only LoRa chipsets on the market are from SemTech Corporation.

The communication on the serial communication bus between the chipset and the CU within the endpoint device is however mostly unencrypted and unauthenticated. A malicious actor with a physical access to the IOT endpoint device can both intercept and modify the communication as well as issue unauthorized commands to the LoRa radio.

Furthermore, almost no devices are secure against side channel attacks. In side channel attacks, information is derived by observing the environment in which the asset under attack operates. For example, by intercepting the electromagnetic emanations or power consumption, and other hardware characteristics of the endpoint device when calculating keys or performing cryptographic operations could be used by attackers to calculate the keys or find out details about the communication. Session keys in the endpoint devices are most commonly stored in EEPROM memory which is known to be vulnerable to side channel attacks [65].

4.8.4 Possibilities for Insecure Implementation of Counters

If the endpoint or server device does not implement or incorrectly implements counter management, this could lead to replay attacks.

The LoRaWan protocol defines uplink and downlink frame counters in the communication. A communication that does not increment a previously used frame counter should be disregarded according to the protocol. The frame counters are secured with a message integrity code to prevent unauthorized modification. Frame counters are reset with each endpoint device activation. At that moment new keys are also renegotiated and old keys are invalidated, which prevents attacker from resending previously recorded message.

Secondly, counters are important for the security of the encryption, as they are used in generation of the keystream for the AES cipher which is XORed with the plaintext message. In case a counter is not implemented correctly, this would lead to a situation where the same keystream is used for encrypting different messages. This could be used by an attacker that can intercept messages to calculate the keystream, and thus also decrypt the communication [65].

4.8.5 Weak Implementation of Random Number Generators in Endpoint Devices

In order to ensure security of the endpoint devices, they must be able to generate cryptographically sound (pseudo)-random numbers using. During the over-the-air activation of the device, the endpoint needs to generate a random DevNonce, which is then sent to the server and used both to prevent replay attacks and generate session keys. DevNonce is sent unencrypted and it is therefore very important that it has been created with strong pseudo random number generating function (PRNG).

Experience tells us that creating strong and secure PRNG is a difficult task. In the context of IOT consumer devices, this is further compounded by the fact that these devices are operating in low-power and low-performance mode.

Research has been conducted where LoRa chipsets available on the market were tested for strength of the PRNG using statistical tests. Two scenarios were considered, one where the performance of PRNG is measured in the absence of attacks, and second experiment where performance was evaluated in presence of an active jammer that disrupted the signal and influenced the input variables which are used to calculate the random number. In both cases, results have shown that the PRNG exhibits weaknesses and that there is a bias generated pseudorandom number values [54].

In worst case scenario where the generated DevNonce value is identical each time due to a high saturation of the signal and no randomness in the PRNG function, the end device will be susceptible to denial of service.

The DevNonce will be the same each time the endpoint device initiates the join request activation procedure, which will in turn be ignored by the network server in line with replay protection measures.

The LoRaWan protocol specification gives limited guidance about how should the PRNG be implemented.

4.8.6 Possibilities for Unencrypted Control Information

The protocol allows two options for exchanging administrative MAC commands between endpoint devices and network servers. Either inside the frame payload where such commands are inherently encrypted, or by piggybacking on regular communication in the FOpts field. Disadvantage of using the FOpts field is that those commands will not be encrypted, and it is left for the developer to make sure that case sensitive MAC commands need to be shared FOpts field is not used.

A potential improvement would be to encrypt the FOpts field with the NwkSKey session key.

4.8.7 Out of scope for Vulnerability Assessment

This list was not encompassing. We focused on vulnerabilities that are directly related to the specification of the LoRaWan protocol, its implementation by network carriers and device manufacturers, as discussed in Chapter 1.

Many vulnerabilities lie on the border between the wireless network and the endpoint or server-side devices themselves. These were in most cases not considered and are subject of further research. This paragraph lists a few of these border cases where many vulnerabilities will certainly occur in the future, to give reader some indication of what is left out.

The session and root keys for the LoRaWan communication will be in most cases stored in the firmware or operating system of the endpoint device. The supply chain and secure software development process for the firmware and operating system is thus important, but out of scope for this research.

The server-side applications processing data received over the LoRaWan network from the endpoint devices need to take many security measures in place. First of all, although the endpoint devices are authenticated, communication is encrypted and protected for integrity, the servers cannot trust the correctness and validity of the data and should perform input validation for attacks such as injections, remote code execution, and malware spreading. Furthermore, each data input should ideally be logically validated for the right syntax. Endpoint devices will always be compromised, for example by a legitimate customer who decides to change the behavior of the endpoint to a malicious one.

Some parts of the IOT ecosystem, typically on the server side of the network operator, will be connected to the Internet. The owner and operator of these parts of the ecosystem must take care that they are secure and adhere to standard security requirements for Internet connected components. This includes attacks against confidentiality, integrity and availability, which have been widely discussed in the literature.

Both the network operator, application owner, and device manufacturers have their piece of responsibility in implementing security in the software stack. Starting from implementation of the AES128 protocol in the LoRa chips, over to proper implementation of validation of the MICs, encoding of the communication, recovering from errors in the communication on all layers and malformed communication packets, to things such as taking care that sensitive information is not logged in volatile or permanent memory of the devices, intrusion prevention and detection system on the network provider side, backups of both configuration as well as distributed session keys, and performing regular security penetration tests.

For a more complete list of all requirements that are mandated for various players in the IOT ecosystem, refer to the appendix framework to this research.

4.9 Summary of the desktop research

This Chapter will consolidate results from Phase 1, the desktop research, will draw conclusions.

4.9.1 LoRaWan Specific Vulnerabilities and Countermeasures

We identified 18 low-power wide area (LPWAN) network specific countermeasures that each LPWAN protocol should implement. An analysis of the LoRaWan protocol version 1.0.2 class A identified that out of the 18 countermeasures, 8 were attempted to be solved in the protocol, and 10 were not. We further studied the protocol in order to identify vulnerabilities in the design of those 8 countermeasures that were considered in the protocol. We noticed vulnerabilities in almost every countermeasure that the protocol attempted to implement. We also identified cases where the protocol leaves room for the device manufacturers and network operators to interpret or ignore the specific countermeasure thus leaving room for additional vulnerabilities. These conclusions are summarized in Table 5. First column shows requirements prescribed to LPWAN networks by the industry to mitigate existing threats. Column 2 shows if the requirement is implemented in the LoRaWan protocol specification. Column 3 shows if there are known design vulnerabilities in the protocol in case the requirement was considered. Column 4 shows if there are additional vulnerabilities that could arise from wrong implementation of the requirement.

The specific security implications that this situation of leads to (i.e. consequences of not mitigating a certain threat) are well understood by the industry, discussed thoroughly throughout the thesis, and partially obvious from the table itself.

Table 5: LoRaWan specific Vulnerabilities and Countermeasures

Countermeasure Requirement	Implemented in LoRaWan?	LoRaWan vulnerability due to poor protocol design	Possibility for Implementation Vulnerabilities
4.5.1 Existence of Global Unique Identifiers	Yes		
4.5.2 Authentication of device, subscriber and network	Yes	4.7.1 Insecure Device Activation Option	
4.5.3 Privacy-Preserving Identity Protection	No		
4.5.4 Data Confidentiality	Yes	4.7.4 Decryption of messages for ABP devices 4.7.11 Bit-Flipping Attack	4.8.4 Possibilities for Insecure Implementation of Counter 4.8.6 Possibilities for Unencrypted Control Information
4.5.5 End-to-Middle Security	Yes		
4.5.6 Forward Secrecy	No		
4.5.7 Integrity Protection	Yes	4.7.10 Message Integrity Code subject to Brute-force Attack	4.8.2 Possibilities for further Attacks on Message Integrity
4.5.8 Replay Attack Protection	Yes	4.7.3 Vulnerabilities in Design of Counters 4.7.2 Vulnerabilities with OTAA and DevNonce 4.7.6 Wormhole Attack	4.8.4 Possibilities for Insecure Implementation of Counter
4.5.9 Reliability of Delivery	No		
4.5.10 Existence of Access Classes for Critical Infrastructures	No		
4.5.11 Updatability of Device	No		
4.5.12 Updatability of Keys and Algorithms	No		
4.5.13 Network Monitoring and Filtering	No		

4.5.14 Key Provisioning	Partially (OTAA only)	4.7.7 Missing Process for Key Management 4.7.8 No Layer Independence for Key Generation in OTAA	4.8.3 Possibilities for Insecure Key Storage
4.5.15 Ability to Negotiate Cryptographic Algorithms	No		
4.5.16 Resistance to Class Breaks	Yes		4.8.1 Possibilities for Insecure Key Generation
4.5.17 Requirement for Mandatory Device Certification	No		
4.5.18 The Ability to Layer IP Protocol Over the LPWAN Protocol	No		

There are further additional 3 vulnerabilities which even if all identified countermeasures were implemented would not be mitigated, these are:

- 4.7.5 Vulnerability to Radio Jamming
- 4.7.9 Gateway and DDOS
- 4.8.5 Weak Implementation of Random Number Generators in Endpoint Devices.

4.9.2 IOT Frameworks and The State of the Art in the Industry

The described methodology was followed to study existing industry IOT frameworks, and to classify threats and countermeasures in order to arrive at a set applicable for our use case (security of consumer-grade IOT LoRaWan connected products).

The outcome of this process is that the studied industry frameworks would not address many of the known LoRaWan-specific vulnerabilities and prescribed mitigating counter-measures.

Table 6 summarizes the result. The first column shows mitigating counter-measures that are known to mitigate existing threats in long range wireless protocols such as LoRaWan. The second column shows whether the countermeasure is covered in at least one of the industry frameworks. The third column shows whether at least the threat related to the counter-measure is known in the industry frameworks. References to the chapters in the thesis are given.

Table 6: Comparison of Practice and Theory for recommended countermeasures

Expected Countermeasure	Countermeasure available in the frameworks	Known Threats in Industry Frameworks related to the countermeasure
4.5.1 Existence of Global Unique Identifiers	4.4.7 Identification on the Network	
4.5.2 Authentication of device, subscriber and network	4.4.4 Protection against Unauthorized Connections	4.3.4 Unauthenticated or Unauthorized Communication
4.5.3 Privacy-Preserving Identity Protection		
4.5.4 Data Confidentiality	4.4.1 Encryption of the Communication	4.3.1 Eavesdropping of messages
4.5.5 End-to-Middle Security		
4.5.6 Forward Secrecy		
4.5.7 Integrity Protection		4.3.2 Alteration of Messages
4.5.8 Replay Attack Protection	4.4.3 Replay Protection	4.3.3 Replay of Messages
4.5.9 Reliability of Delivery		
4.5.10 Existence of Access Classes for Critical Infrastructures		

4.5.11 Updatability of Device		
4.5.12 Updatability of Keys and Algorithms	4.4.5 Secure Key Management	
4.5.13 Network Monitoring and Filtering	4.4.2 Firewall	4.3.5 Lack of Network Isolation
4.5.14 Key Provisioning	4.4.5 Secure Key Management	
4.5.15 Ability to Negotiate Cryptographic Algorithms		
4.5.16 Resistance to Class Breaks		
4.5.17 Requirement for Mandatory Device Certification		
4.5.18 The Ability to Layer IP Protocol Over the LPWAN Protocol		
N/A	4.4.6 Network Resilience	4.3.6 Loss of Connectivity to the Network

4.9.3 Conclusions from the desktop research

In this chapter we asked the following question: what are the known cyber security threats, vulnerabilities and recommended counter-measures?

To answer this, we provided a comprehensive list of threats, vulnerabilities and mitigating measures that can be considered by manufacturers, network operators, and in the future improvements of the protocol. Such a comprehensive overview has not been to-date published.

The first phase of the thesis, which took form of a desktop research, also conclude the following two statements that will require further investigation:

a) **LoRaWan is risky**: 18 specific countermeasures exist that mitigate threats for technologies such as LoRaWan. In the design of the LoRaWan protocol version 1.0.2 class A, 10 out of those 18 countermeasures are not considered. For the remaining 8 that are considered, at least 5 are not designed well and are vulnerable.
b) **Frameworks do not address all risks**: The existing IOT frameworks from the industries cover 7 out of the 18 known countermeasures, and therefore only mitigate part of the threats. The remaining 11 are not covered in the frameworks.

5 Phase 2: Stakeholder Interviews

5.1 Research questions for the expert interviews

The first phase of the thesis, which took form of a desktop research, concluded the following two statements that require further investigation:

c) **LoRaWan is risky**: 18 specific countermeasures exist that mitigate threats for technologies such as LoRaWan. In the design of the LoRaWan protocol version 1.0.2 class A, 10 out of those 18 countermeasures are not considered. For the remaining 8 that are considered, at least 5 are not designed well and are vulnerable.

d) **Frameworks do not address all risks**: The existing IOT frameworks from the industries cover 7 out of the 18 known countermeasures, and therefore only mitigate part of the threats. The remaining 11 are not covered in the frameworks.

To provide context to the above two conclusions supported by details from Phase 1, a qualitative study was conducted. The study will address the following research questions related to the above conclusions.

1) **Root cause**: How do you explain the conclusions?
2) **Impact**: What impact does that have on consumers?
3) **Recommendation**: Should we do something about it and what?

This chapter summarizes the most important outcomes of the expert interviews. Each section states the codes and interviewees that mention the code. An example citations from the transcripts are mentioned. The section then follows with interpretation, and conclusions.

5.2 Roles and Responsibilities

Most interview participants stated that the responsibilities in the LoRaWan consumer product landscape should be split as follows.

5.2.1 LoRa Alliance (protocol designers)

Code	Interviewee	Citation (Example)
11) LoRa Alliance Responsibilities	C, E, F, H, G, L	H: "It might be the effort for the Alliance to host an environment - a repository of frameworks". J: "The decision [about how much security to include into the protocol] will be ultimately to the designer of the protocol, he is the only one who can make the decision." L: "LoRa Alliance chose a level of how secure the protocol is going to be, trying to find a reasonable balance. If they implement more security, you will be able to use LoRaWan for different purposes. If you have low security then certain possibilities are not going to be possible, because you don't have enough security in the protocol."
2) Business vs. Security in LoRaWan	B, C, D, F, H, I, J	C: "That's the devil's dilemma between the battery consumption and the security of the devices."

The LoRaWan protocol designers, LoRa Alliance, face a decision about which security threats to mitigate in the protocol specification and to what degree. This is a devil's dilemma; if a certain counter-measure is not included in the design of the protocol, this will in many cases lead to blaming & shaming of the protocol makers from the security industry. If on the other hand, as many security threats as possible are mitigated, this will make the protocol less usable, and will lead to criticism from the engineers and product manufacturer's corner. The solution is to be completely transparent about the design choices and which threats were mitigated and how, and which weren't and why.

Most security measures come with a cost. Either in the form of time needed to properly design and test the measure and thus delay the release of the protocol specifications. Or in the form of additional requirements on the protocol implementers and end devices manufacturers. Additional requirements might increase the production cost and energy consumption of the end devices up to the point that the LoRaWan protocol stops being useful.

A conscious choice thus needs to be made about where to draw the line and which counter-measures should be mitigated. This is the responsibility of the LoRa Alliance to draw the line based on the use cases for which the protocol was designed, and the expected impact of the implemented countermeasures on the whole ecosystem. In order to prevent future blaming, LoRa Alliance must to be open about the class of use cases for which the protocol is secure enough and for which it not. Ideally, such risk assessment should be published openly alongside the standard.

We cannot be expected that all network protocols mitigate in their design all security risks, especially not protocols such as LoRaWan designed for low power communication which inherently calls for simplicity in the implemented countermeasures. We should thus also not blame the LoRa Alliance for not mitigating certain risks as long as LoRa Alliance is transparent about what were the design choices behind the protocol, and which risks are not mitigated.

5.2.2 LoRaWan network operators

Code	Interviewee	Citation (Example)
7) Network Operator Responsibilities	B, C, E, I, J, K, L	C: "Network operator is responsible for the network security, because it's their network. They should do a strong assessment before deploying the network."
4) Business vs. Security in Network Provider	A, C, L	L: "Network providers operate on what they can monetize. If most of the manufactures don't need a security feature and it is an expensive measure then they probably won't implement it. If they think that lots of manufacturers will need this feature, then it will be interesting for them to add to the network."

The network operators implement the protocol and operate the LoRaWan gateways for the consumer market, typically in form of large-scale deployments. Their responsibility is to implement duly the protocol specifications. Similarly, as the LoRa Alliance should be open about the design choices behind the protocol and which risks are mitigated, the same holds true for the network operators.

Network operators are responsible for performing a security test to validate robustness of the implementation. Each class of use cases come with different risks, and it is not fair to expect that network operators will voluntarily implement additional measures to address risks that were not mitigated by the protocol designers. Network operators will behave economically and can if they wish so address a gap in the ecosystem by offering additional mitigating measures for additional fees, either hidden or explicit.

5.2.3 Consumer Device Manufacturers

Code	Interviewee	Citation (Example)

6) Manufacturer Responsibilities	A, C, D, E, H, J, L	L: "Manufacturer is a professional organization that knows what an IOT device is going to be used for. They are in the best position to make this call [about how much security to put in the product]". J: "If manufacturers make a decision and say: this decision [about security] is made because of these reasons and publish that, then no one will blame them in case a conscious decision was made not to implement strong security".
3) Business vs. Security in Product	A, B, C, D, E, F, H, I, J	B: "So in the end the trade off will always be done by the persons manufacturing the device. If you have a protocol that drains a lot of energy, you just take a different protocol" .

Manufacturers introduce to the market consumer IOT devices. These are typically created and marketed with a specific use case in mind. The manufacturers have professional duty to perform a security risk assessment of these use cases in order to produce devices that do not pass too many risks onto the consumer.

However costly this might be, the manufacturer owns the business case, profits most from the success of the product, and is a professional organization that is closest to being able to assess the in the product. If manufacturers do not have sufficient knowledge for such a risk assessment, they need to obtain help from a specialized third party that can help with performing such a risk assessment.

Manufacturers eventually decide whether LoRaWan is a technology that sufficiently mitigates the risks associated with the intended use cases, based on facts such as what type of data will be transferred over the network, how sensitive is the data, whether the use case is interesting for any type of attackers, and what class of consumers they aim to market the product to. This is a natural choice, since the manufacturers have the most information about the device or product, its inner working, and can freely decide what technology will be used and how. They are the ones that can mitigate certain risks on the design level, and chose technology that is a fit-for-purpose for the specific use case.

In no situations can all risks be mitigated completely, and zero days cannot be eliminated. Manufacturers should be open about the residual risks that consumers bear. Devices should be designed securely from the beginning in such a way that risk for consumers are limited if they follow the use case for which the device was manufactured. Manufacturers should be responsible for losses and harm to their customers. This could be enforced either by direct claims from consumers, or via regulatory fines.

5.2.4 Consumers

Code	Interviewee	Citation (Example)
5) Consumer Responsibilities	A, C, E, F, H, I, J, L	A: "The consumer needs to be aware. If you have a secure configuration option, they should configure it in a secure way, just like they look their doors."

Consumers are the most diverse group, which is hard to further categorize, they come in all ages, technical skills, awareness of societal problems, and intelligence.

In all cases, consumers are expected to maintain certain security baseline and follow basic security principles, such as password management practices. Unfortunately, such security baseline for IOT devices, and especially LoRaWan products has not yet sufficiently evolved.

We should however not expect that consumers will be able to understand the risks and we should also not hold them responsible for security hardening beyond the very basic security baseline. Ideally consumers should also be critical about the products they buy, and they should demand from manufacturers information whether they performed their risk assessment and what the residual risks are. Never ending awareness is necessary to achieve this point.

In general, consumers should be able to trust that the professional supply chain behind the product (the protocol designers, manufacturers, network operators, and regulations) has performed the due diligence, and that the government has created a system of incentives that ensures that the product on the market is secure enough.

5.2.5 Academia, Researchers, and Consultants

Code	Interviewee	Citation (Example)
8) Academia Responsibilities	A, C, E, H, I, J	A: "Academia is effective if they are not only in their ivory tower doing research but they also have a role in the public debate. "
10) Consultants & Experts	A, B, J	A: "As security professional if you start on the table with the innovators and directly start giving all those lines: it's insecure, but no solution that suits the business case, you will not be invited to that table anymore. "

Academia, independent researchers and consultants have two roles. On one hand, they are responsible for publishing theoretical results, such as research of new threats, vulnerabilities and countermeasures. That is a role they have been always fulfilling well.

On the other hand, they need to be able to participate in a public debate about the practical implications of the theoretical results. Stating a problem (threat or vulnerability) becomes much more valuable if we also have a discussion about the consequence and real impact of the problem. Next to that, researchers are expected to come with a practical solution for the problem that is accepted by the whole community and explain consequences of the solution. The experts expressed that in many cases, this role is not fulfilled sufficiently.

Specifically, publishing that the LoRaWan protocol is vulnerable to a certain attack should come with a discussion whether the attack is practical, to which use cases it applies, what is the impact of a potential attack, whether the vulnerability can be mitigated and how while still having in mind the original use cases, or whether the cost of mitigation is something that we are fine paying for. The fact that LoRaWan is introduced to the market comes with security risks, but the fact that all security risks are mitigated will mean that no such network will ever be possible. This is a step that is often forgotten in the discussion by security experts.

5.2.6 Awareness and Media

Code	Interviewee	Citation (Example)
9) Awareness People Responsibilities	A, B, C, E, J	A: "Journalists write about security and translate the real technical stuff to something a bigger audience can appreciate. That is also important."

		E: "Maybe it's like with the ecological products. Look at that."

Awareness activities by journalists that translate academia results to a wider audience, and by community activists are necessary. Consumers should be educated about their responsibilities, and only a persistent and clear message works.

The security industry could take example from the biological food supply industry, where we managed to change perception of some consumers and convince them to pay more for products that look the same, but where certain health risks are minimized. Recently, we have also started to see that some consumers select their mobile phones and computers based on how well the vendors are known to protect customer data and deal with privacy problems. This additional pressure from consumers will in turn demand manufacturers to invest into risk management activities, and implementation of risk mitigating counter-measures.

5.2.7 Regulation and Government

Code	Interviewee	Citation (Example)
20) Regulation	A, B, C, D, E, F, H, I, J, L	E: "We need a third party there, right? Not LoRa Alliance, because then they are assessing their own protocol, and they are setting a standard and then complying with it."

Finally, all interviewees agreed that there is a room in the ecosystem for another party. On one hand, she could serve as a regulator or guardian of the ecosystem, and on another hand as someone providing objective security-relevant information about the ecosystem. There is a need to compare various protocols against each other and give manufacturers enough information to select the right protocol for their use case. This comparison cannot be done directly by the protocol designers themselves, as they often do not have the insight in competing protocols, lack the objectivity or any economic incentive to perform an objective comparison.

Interviewees agreed that academic research cannot be detached from the rest of the ecosystem. Only the biggest companies such as international corporations having resources to access academic results, translate them into understandable results and take follow-up actions. Media do not sufficiently fill the gap, especially not in less mainstream areas such as IOT. Awareness activities are never sufficient and can accommodate more efforts. We will discuss the regulatory aspect in the following paragraphs.

5.3 Risk assessment of LoRaWan

5.3.1 On severity of threats and risks

Code	Interviewee	Citation (Example)
12) General threats, vulnerabilities, controls	A, B, C, D, E, H, I, L	F: "Choose the protocol based on what kind of data you are sending over it. You shouldn't maybe use LoRaWan network for highly sensitive medical data and you shouldn't use it also for banking. However, it would be fine for some random public data." D: "One of the things that may concern you is the key management."

		D: "The disadvantage of this technology is that you cannot update it over the air. You can only physically update it at the moment."
13) Design of threats, vulnerabilities, controls	B, H, J, L	L: "The first thing I would be interested to ask for some security advice would be: what are you trying to protect against who? Why is the information that passes through here interesting? Who would want to get to it? Does it ever transfer interesting information?"

The theoretical part of this thesis identified a number of threats that are not mitigated in the LoRaWan protocol design, and number of threats that are mitigated partially using vulnerable countermeasures. The expert interviews aimed to explore whether this is a problem or not.

The clear answer from the expert interviews is that each individual threat or vulnerable mitigation can be a problem if the LoRaWan protocol is used as a technology in the wrong business use case. We will present seven examples.

Firstly, we already explained how signal jamming can be used to exploit the technology when used in burglar alarms, effectively disabling the main business use case for which the technology was used in the first place.

Secondly, wormhole attack in combination with other vulnerabilities in the replay protection measures could be a problem if LoRaWan-connected devices would be used as main technology to reliably track people, for example convinced criminals when on a temporary leave from prison. One can imagine a situation where the convict intercepts the message when at an allowed location. This recorded message could later be replayed in combination with jamming of the legitimate signal in case that the convict is located in an area which he is not allowed to visit.

Thirdly, the inability of the protocol to sufficiently support device firmware and software updates was stated by many as one of the biggest limitations of the protocol, not only in terms of security, but also in terms of general viability of the protocol to meet basic business requirements. Vulnerabilities are discovered on daily basis, and the inability of the manufacturer to deploy patches over the air limits many use cases. One can imagine a situation where default administrative passwords are hardcoded in the firmware of the device and this becomes a public knowledge, or where the device firmware is found to be vulnerable to remote execution attacks over the LoRaWan network. The only possibility for the manufacturer in such a situation is to physically replace all endpoint devices, which in many cases is neither economical nor practical.

Fourth, vulnerabilities in the area of data confidentiality would be a problem if LoRaWan was used as a protocol to exchange classified governmental information, or sensitive corporate information without additional level of encryption. Although these vulnerabilities are not easy to exploit, such a scenario would give attackers enough motivation to invest into developing a viable attack.

Fifth, vulnerabilities in the area of key provisioning, and the inability to update keys and algorithms would present a problem if LoRaWan was used in banking for transaction such as payments. Security of many transaction mechanisms is based on the trust in cryptographic keys. The ability to rotate these keys frequently is an important requirement.

Sixth, and finally, the fact that the protocol does not implement controls that would ensure reliable delivery means that it would be a bad choice for certain use cases; for example, as a technology in train control and monitoring systems. In case that LoRaWan connected devices would be used to monitor which rail is occupied and inform operators in case that a train entered a wrong rail, one undelivered message, or late delivered message could have fatal consequences.

As a conclusion, we discussed seven threats and associated scenarios identified in the earlier chapters of this thesis. For each threat, we managed to identify a realistic use case where the threat would present a major problem if the use case was introduced to the market in the form of a consumer product. That has already in some cases happened. It was not possible, given the wide background of the experts, their familiarity with the LoRaWan protocol, and the number of threats that are theoretically known to discuss them all one by one in detail.

The next chapter will discuss which class of use cases are suitable for the LoRaWan technology.

5.3.2 Use cases for LoRaWan

Code	Interviewee	Citation (Example)
14) Use case for LoRaWan	D, F, H	D: "If you see LoRaWan technology just as an environmental sensor where not much harm is done if it is somehow hacked. The worst that can happen is that you get wrong temperature data in your database. OK, who cares." F: "If you want to have a secure IOT product, and if you want to use a low memory, low CPU, then you maybe made the wrong design decision in the first place." L: "It's harder to monetize the location tracking".

The previous paragraph discussed in detail use cases that are not suitable for the LoRaWan technology due to the inherent threats and vulnerabilities in the protocol design. The remaining question thus is which use cases are suitable for LoRaWan?

The interviewees unanimously agreed that there is a space on the market for a range of protocols. Some protocols will be aimed at solutions with high security concerns, and others at solutions where security is less important. Security always comes with a cost, and hoping for high security while meeting all other business requirements is too naive. LoRaWan class A is primarily destined for solutions where long range communication and low energy cost is a requirement. It is expected that the protocol will be deployed in low cost devices operating on battery, where the sensitivity of transferred data is limited.

A wide consensus was reached that LoRaWan class A connected devices should be primarily used as sensors measuring non-sensitive non-personal parameters of the environment in which they are operating. A good use case would be temperature, humidity, pollution or noise level sensors not only for consumers, but also for government (smart city setups) and industries. Such setups are less sensitive on the security of the communication. The build-in measures in the protocol are good enough to provide sufficient level of security to the ecosystem. A good example are sensors used by farmers in agriculture to count their assets and provide early warning systems.

Second category of use cases are sensors that report personal information about the consumer, such as location, medical-related data or performance of various daily activities. Whether the protocol is sufficiently secure for such a setup depends on the specific use case, the sensitivity of the connected data, and the risk that the consumer is willing to take. Some interviewed consumers did not consider their location as a sensitive value, while others did.

All interviewed experts and consumers agreed that connecting medical devices to LoRaWan would not be possible while sufficiently mitigating the risks. Vulnerabilities could be used to extort consumers and institutions, and in the worst case lead to a harm or death of consumers.

Using LoRaWan connected devices for solutions with availability requirements, or where security considerations are high should be avoided. Example of these are banking systems, systems that themselves provide security (physical or virtual), or systems that collect very sensitive data, or execute important decisions. Designing a product over the LoRaWan technology that is hard to hack and exploit is a very difficult tasks with limited research and guidance currently available.

Then next section explains the LoRaWan ecosystem from attacker's point of view.

5.3.3 Attacker's perspective

Code	Interviewee	Citation (Example)
15) Attack vectors & actors	A, B, C, E, F, G, H, I, L	J: "A criminal looks at a solution and then says: aha - I can make money out of that. He does not start thinking - how will someone design something that I can make money out of" L: "Script kiddies are mostly a local threat." L: "Having LoRaWan connected burglar alarm is sensitive, because criminals LoRaWan might be used if to figure out there is burglar alarm in the first place, if it is on, that sort of info. The use case for the type of device really matters if you would care about security of it. If it is just measuring the temperature and communicate it to a central point. Nobody is going to attack it."
16) Impact of attack	A, B, E, F, G, H, I, J, L	E: "For now I would not be too afraid, depends of course on the device, but I don't really see possibilities to monetize"
17) Defense mechanisms	A, H, L	A: "I have seen firewalls for IOT, that is Wi-Fi based, I have not seen any for LoRa or ZigBee. "

The vast majority of attackers have a motive for their actions. In the interviews a number of actor groups were discussed separately with the following conclusions.

Individual criminals and organized crime is looking primarily for ways to monetize the attacks, for example by stealing money, stealing data, or building a platform for consequent attacks.

The LoRaWan IOT ecosystem is not secure enough to serve as an infrastructure for financial transactions such as payments. The root cause is the fact that LoRaWan protocol aims at low power devices where costly mitigations are not an option. Insufficient protection in the design of the protocol against replay attacks, non-repudiation, and integrity protection leaves a lot of room for attacks on transaction systems.

LoRaWan-connected devices should also not be used as access controls to other networks or physical spaces. The protocol cannot guarantee availability and is subject to jamming. It is therefore a mistake to use LoRaWan devices in solutions where availability of the communication is a requirement. LoRaWan connected burglar alarms and home connected security systems have already been introduced to the market. The vulnerabilities in the LoRaWan protocol help attackers to identify exact location of these alarms, possibly further identify whether they are on or off (thus telling the attacker if the owner of the property is in or not).

Attackers would also be able to jam the signal with off the shelf hardware and thus render the burglar alarms useless.

Similarly, as in the early days of the Wi-Fi technology 802.11 access points lead to many attacks on local area networks, the ethical hacking community expects that only time will take until vulnerabilities are discovered in gateways and home-connected devices that will allow attackers to pivot further to IP-based networks.

Stakeholders did not come to a consensus whether the growing number of LoRaWan connected devices can ever be turned into a platform controlled by attackers and used for further attacks. Connectivity to the devices over LoRaWan is only possible when in the vicinity of the devices, and some believe that the very limited bandwidth and low computing power of most of the devices make them less attractive to such attacks. Other expressed the sheer number of such devices and interconnectivity will eventually lead to class breaks and emergence of LoRaWan-connected botnets.

Most experts believe that LoRaWan devices have privacy concerns. One of the threat actors are nation states. Over the last year, on multiple occasions we have learnt that governments are interested in collecting data about citizens. Since LoRaWan operates in the public radio frequency spectrum, nothing stops governments from installing their own gateways across the country to monitor movements of devices, where devices are often associated with their owners. Although the payload of the messages is encrypted end-to-end, many argued that the metadata is more interesting to nation state actors that the data itself. Nation state actors can also obtain such information directly from the network operators. Other threat actors to privacy of consumer are private entities such as detective agencies, or even employers or partner entities trying to track others. Some LoRaWan networks operate on community basis, where network gateways are operated by individual contributors to the community. These could also be run by actors with malicious intentions who want to collect data about consumers and use it as a stepping stone for further attacks. Separate book could be paid to privacy-related concerns in IOT devices. This aspect is out of scope for this thesis.

None of the interviewees mentioned that he would have heard of attacks "in the wild" that would exploit a vulnerability or unmitigated threat in the LoRaWan protocol. This has two possible explanations. The first theory is that the technology is too young and attackers are focusing on IP-based network, where the return on investment as well as possibilities to monetize are higher. This is supported by the general feeling in the LoRaWan community that the solution is rather mature, but the number of solutions making use of the technology is very limited. In contrast to this are generic statistics from network providers stating that millions of devices are connected existing LoRaWan networks. The second possibility is that attacks are happening and we do not know. Possibility there exists consumers who are getting harmed, for example a house of a consumer is robbed by attackers exploiting vulnerability in the burglar systems. However, unless we find a way to connect the impact of the attack (e.g. burglarized house) to the vulnerability in the LoRaWan connected device, the existence of these attacks will not be attributed to LoRaWan. Network operators at moment in many cases do not monitor performance and behavior on the network and cannot confirm or dispute this fact.

Other attack vectors mentioned were botnet creation for (distributed) denial of service attacks on the network itself, and possibility for ransomware, although not agreed by all experts.

Defense mechanisms, such as firewalls or intrusion prevention/detection systems currently do not exist. Most experts see that this will be eventually introduced to the market.

5.3.4 The bigger picture

Code	Interviewee	Citation (Example)

36) The bigger picture	C, I, J	I: "The biggest security challenges are not with the LoRaWan security, but with the network operators and product manufacturers' security." J: " you cannot design the protocol in such a way that it will be useful for everything. The most you can do there is design it as robust as possible and then be very explicit in what the design principles were." C: "I would always attack the application server. Always. Because the application server owns all the session keys."

The interviews emphasized that as much as the security of the network protocol is very important, maybe even more so is the security of the remainder of the ecosystem.

No matter how strong the network design is, the stakeholders mentioned that the biggest risk in the ecosystem is in the security of the backend systems connected to the IP networks, and the operational security.

Endpoint device manufacturers are of the opinion that performing a successful and scalable attack (i.e. an attack which spans more than one LoRaWan device) will require significant more effort than exploiting either LoRaWan network provider or application back-end servers. Keeping up with the ever-changing threat landscape of an Internet-facing application as an application owner is more important that focusing on vulnerabilities in the LoRaWan protocol and worth paying attention in the first place.

The interviewed ethical hackers and network operator representatives confirmed that from attacker's point of view who is trying to monetize her efforts it will be more cost-beneficial to attack backend servers that store the root or session keys for the associated endpoint devices, or directly attack application or database servers where data is processed and stored. These will be in almost all cases traditional IP based systems with widely known vulnerabilities and readily available exploits.

Assuming that the design of the protocol and its implemented by the network operator and devices manufacturers is security, risks will always remain elsewhere. Focus should not be on meticulously eliminating all theoretical problems in the LoRaWan design. One interviewee mentioned a third party he is cooperating with, which processes LoRaWan private keys by mailing them in plaintext over email. These are not the things that will be covered in many frameworks or academic research, but the ones that will be in reality often misused by attackers.

5.4 Problems in the LoRaWan ecosystem

The IOT LoRaWan ecosystem suffers from a number of problems. Some of these are widely known and not unique to the ecosystem, but, the nature of the LoRaWan IOT ecosystem accentuate the problem. Others are rather unique. These problems were brought by more than one expert as part of the interviews.

5.4.1 Information Asymmetry between consumers and manufacturers

Code	Interviewee	Citation (Example)
27) Information Asymmetry	C	C: "There is information asymmetry between the users and the manufacturers, and also between the manufacturers and the LoRaWan alliance, and I think that should be aligned more. "

		C: "If the users don't know that threats exist, but the vendors do but it is hard to mitigate those threats, but then I will chose as a vendor to accept those risks, because the users don't know."

An information asymmetry exists between consumers and manufacturers of the devices. Consumers are not aware of security threats and risks associated with the products they buy, and therefore are often not willing to pay more for products that mitigate these risks. Vendors as a consequence do not have incentives to implement security, and will decide to accept the risk associated with selling insecure products. Mitigating risks costs time and energy, which will be reflected in the price of the product, and could paradoxically lead to the product not being successful on the market. This phenomenon is also known as the lemon market.

5.4.2 Limited experience with security among device manufacturers

Code	Interviewee	Citation (Example)
24) Knowledge of product teams	B, C, E, F, H, J	F: My main concern is that developers with no security background will start using LoRaWan to broadcast sensitive data.
35) Drawing Parallel	B, C, H, J	E: Philips Hue designed security nicely because you have to associate keys which is a difficult process for end users, so they decided it needs to be user friendly, because otherwise nobody is going to use it.

Majority of the interviewed experts expressed as one of their biggest concerns in the IOT LoRaWan ecosystem a lack of knowledge on the manufacturer side. IOT industry attracts many startups and young innovators with background is software development and hardware engineering. Most of them have limited background in cyber and information security, and not enough means to hire specialists with in-depth knowledge of security and privacy topics. Technology is often being put central, with use cases built around technology, and products being built around these use cases. This is supported by the LoRaWan community that in many community meetings spreads a message that the technology is ready and should be used for as many use cases as possible. Security experts agree that the use cases should be put first, and only secondary the right technology must be selected based on a risk and impact assessment. This is in many cases not done with security concerns entering the discussion after the technology and use case has been selected. In the moment when it has been decided what type of data will be stored, processed, and transferred and over which technology, the main security risks are given and in many cases have to be accepted by the parties in the ecosystem, if they want to use the product.

One of the common misconceptions among manufacturers not experienced with computer security is that implementing security will inevitably hamper user experience and reduce the likeability of the product. Existing products on the market showed that a product can be designed securely and user-friendly at the same time. For example, the Phillips Hue light bulbs that use for network connectivity a similar technology called ZigBee have designed the solution in such a way that the key distribution process is controlled via button on the gateway associated with the bulbs. This enhances security of the ecosystem, and has been proven to be both likeable by users and strong from security perspective.

Similarly, as at the side of network operators where strong internal policies and regulatory functions can stop business units from introducing to the market insecure LoRaWan networks, it is widely believed by almost all experts that only regulation can stop manufacturers from introducing to the market products with not-acceptable risks. This is discussed in the next section.

5.4.3 Lack of incentives for network operators to secure the networks

Code	Interviewee	Citation (Example)
31) Insufficient incentives	A, C, E, H, L	C: "In the beginning we weren't aware at all about security. We just wanted to launch. Because of the network externalities, launch and fix later"

Network operators that implement the LoRaWan protocol and provide network connectivity to device manufacturers and consumers are also driven by economic incentives. Each network operator wants to be the first that covers a certain geographical area in order to attract devices to connect and benefit from the network externality effect.   However, mitigating security risks comes with additional cost and time requirements that delay the introduction of the network on the market. LoRa Alliance does not provide any guidance about how risks should be addressed, and how the protocol should be implemented. This leads to further delays, and in practice leads to implementations with many of the vulnerabilities. The experts working for network operators confirmed this was the case during the initial launch of the LoRaWan network. Only a strong regulation within the network operators (e.g. strong policy framework and powerful security departments) was able to stop insecure networks from being introduced to the market.

5.4.4 Problems with the LoRa Alliance and the LoRaWan protocol

Code	Interviewee	Citation (Example)
29) Problems with the LoRaWan standard	C, L	C: "What is a missed opportunity for the protocol specification is that it does not have any advice for network operators how to cope with certain threats. They leave it up to the network operators and they don't have any advice. And that is not good." L: "Information should be public knowledge. You would want those sorts of properties to be known so that manufacturer should make their decision: should we focus on speed, or should we focus on security. What fits the product that we are trying to market. Obviously if that sort of information is not out there, and they don't really know the strength or weaknesses of the different protocols that they are comparing to use in their device, then that's a problem.

Applying consequences drawn from the interviews to the LoRaWan ecosystem, a number of issues arrives that should be addressed.

LoRa Alliance is not open enough about the protocol itself, including security measures. The standard is not freely available on the Internet and has to be requested via email, which takes a number of days to respond, in my case 6 days.

There is an information asymmetry between the protocol designers and network operators that implement the protocol. Little has been published by the LoRa Alliance about the use cases for which the standard has been designed, and the associated threats, vulnerabilities and risks. No central repository is available where manufacturers could obtain the threats not addressed in the protocol, or known vulnerabilities in the protocol design. This increases the likelihood that manufacturers will select LoRaWan as a protocol of choice for use cases where higher level of security than the one offered by LoRaWan is necessary. This for example happened in the case of LoRaWan connected burglar alarms where vulnerabilities and features of the LoRaWan protocol may allow attackers to on one hand identify presence of such systems and further give the possibility to jam the signal rendering the such system useless. Nothing on the LoRaWan website will however warn the implementers about the vulnerability of the protocol for network jamming.

On the contrary, the available whitepapers published by LoRa Alliance may give a false impression that the system is perfectly secure. The following statement is available on the LoRa Alliance website: "as shown in this paper, the LoRaWan specification has been designed from the onset with security as an essential aspect, providing state-of-the-art security properties for the need of highly-scalable low power IOT networks." This can easily raise a false impression that all security risks are mitigated and that solution is secure for any deployments.

Besides not being completely open about use cases and risks, the LoRa Alliance also does not give any guidance to the rest of the chain about how to deal with the risks inherent in the protocol. Many gaps that the protocol does not address are left to be dealt with by the network operator, manufacturer or even consumer. Two biggest security concerns that most experts mentioned are the lack of mature key management, and the inability to properly update the endpoint devices over the air. Protocol designers are in many cases aware of many of the security risks, but are not motivated to openly publish them to drive the adoption of the protocol in short-term among network operators and implementers.

5.4.5 Problems with the role of academia and security professionals

Code	Interviewee	Citation (Example)
26) Reasonable Security Profession	A, B, J	J: "Assuming that it [vulnerability, threat] will impact the consumer is a big step...". A: "As security professional, do not only tell the cool story: this is what we broke. But also explain what the consequences are and then start to deal with the pressure of the crowd. Because that's the only way how you can get forward, and if the crowd does not want your solution, then you are still right on paper, but that's not a valid solution."

Academia is expected to function among other as a watch dog and guardian of the security. However, the published LoRaWan vulnerabilities are often extremely theoretical and very far from reality. The likelihood of them being exploited is very low, and the impact for most use cases as well. Researchers do not contribute in the public debate. None of the LoRaWan community meetings I was part of was a representative from the academia present.

Interviewed stakeholders expressed a concern that security experts are in many cases unreasonable. The security profession has in the past years too many times come with one-sided arguments about security, mandating that all vulnerabilities are mitigated and all attacks are prevented without providing practical solutions and engaging in a constructive debate. This behavior has reduced the reputation of the profession and lead to situations where researchers and consultants were not invited to the discussion. The society outside the core cyber security community does not expect researchers and consultants to be articulating only risks, and thus slowing down every innovation and progress. There is a silent expectation that the cyber security professionals will be reasonable and will understand that not all risks can be mitigated.

5.5 Regulation

Code	Interviewee	Citation (Example)
20) Regulation	A, B, C, D, E, F, H, I, J, L	A: "If nothing happens then the politicians will over react" H: "It is a good idea to have regulators act. Usually regulation But there has to be a knowledgeable partner helping them setup the regulations."
21) Certification	A, C, D, E, H	C: "But as of yet, there isn't any kind of certification available, there isn't any kind of standard or framework that is generally accepted throughout the complete European Union, and then legislation is very hard. "

It is widely believed that the only solution to solve many of the identified problems, including the information asymmetry, the lack of incentives to invest in risk mitigation, as well as general knowledge of cyber security challenges among the devices manufacturers is by regulation. However, the experts did not agree in how the regulation should look like, which is also thought to be the reason why there has not yet been any regulation introduced so far. Law makers typically act in situations where the market is not able to address the problem itself; that is apparently also so far the case of IOT.

The following conclusions were drawn from the interviews.

Regulation should not be aimed at specific technology. Such regulation is easy to circumvent, e.g. by renaming or altering the technology to fall outside the scope of the regulation. Furthermore, the regulation would not be long-lived in the ecosystem which is changing as fast as IOT.

Regulation should be aimed at responsibilities of different stakeholder in the ecosystem, including the protocol designers, the network operators, the device manufacturers, and potentially also the consumers.

When it comes to regulating the responsibilities of consumers, the industry can learn from the banking sector which in many areas introduced shared responsibility of consumers for their financial losses. In case that consumers did not keep a certain security baseline, and did exercise a basic due diligence, they could be responsible for attacks on their bank account. This could be in situations where a consumer is using outdated operating system, does not use up-to-date virus scanner, or does not change default passwords in his infrastructure. Applying this to LoRaWan could mean that consumers who do not follow instructions in the device manual, do not change default passwords, or do not keep their password secret will not be able to hold manufacturers responsible nor file insurance claims.

For regulating responsibilities manufacturers, GDPR should serve as an inspiration. Introducing on the market devices that do not mitigate certain threats could be subject to penalties or even removal of the devices from the market by authorities. This would mean that manufacturers who do not invest into security can try and introduce to the market cheaper devices, but with the risk that they are banned and not allowed to be sold in the first place.

However, many interviewees expressed a fear that thanks to the quickly changing industry, regulators do not have enough knowledge and understanding of the problem, and that they will introduce a regulation that will be ineffective in addressing the situation, and on top will add additional bureaucracy for the manufacturers and/or network operators. The regulation should be created as a cooperation between law makers and industry experts, and ideally should be connected with industry specific certifications. At the moment, no such certifications exist.

5.6 Frameworks and Gap between Academia and Industries

Code	Interviewee	Citation (Example)
34) Frameworks	A, C, E, F, H, J	F: "Frameworks are difficult. Frameworks can be good, but then you have to set them in different aspect. One is different than the other one and they all have different capabilities" J: "There is a big gap between a theoretical vulnerability and a practical one."

With regards to the second research objective of the expert interviews, i.e. the gap between industry frameworks and threats, vulnerabilities and countermeasures known to the academia: all interviewed experts were little concerned with this gap.

First, the quality of frameworks is questionable, many were published only because various institutions and individuals wanted to be the first to claim expertise in the IOT topic. Their goal was to have a publication in the area of IOT, and less so to have a complete and holistic methodology. Secondly, frameworks were created with a specific problem in mind, and often are set in an implicit context, such as industry, use case, geographical area, and rarely can be applied as a whole. As a consequence, there will always be a need for new frameworks that will be different from the previous ones. Thirdly, frameworks should be considered more as a guideline for various stakeholders. Frameworks should be the starting point for tailored risk assessments, and should rather serve as an inspiration about how others encountered and solved a similar problem, and not as a solution on its own. Fourth, there are not enough incentives to create and openly publish a holistic framework. Publishing and keeping such framework up-to-date requires significant time and skills, with minimum return on investment.

A known problem with academic results is that they often end with an identification of a vulnerability, and do not fully assess the impact and likelihood of the vulnerability affecting the existing IOT solutions. This would justify that not all vulnerabilities known to academia are part of the industry frameworks or that framework authors are not always looking at the academic research as the source of the framework content.

On the other hand, several experts mentioned that translation from academic threats to what adopters of the LoRaWan standard should be doing is a gap, which however is not expected to be solved by the framework authors. Manufacturers will always come with a new way how to use LoRaWan in their solutions and it will remain their responsibility to always assess the impact of the technology on their use case.

Finally, we will discuss whether the most commonly mentioned concern areas for the LoRaWan technology are included in at least one framework.

1) The inability to update the device over the LoRaWan communication was the most commonly mentioned concern. Most frameworks mentioned patch management for end devices as one of the requirements, none however mentioned that this should be a feature of the network protocol to enable patch management over the air. Since the only other option is to patch IOT devices physically, this is clearly a gap in the framework that is not discussed prominently enough.
2) Key management and security of root keys was mentioned in multiple frameworks, and is given sufficient attention.
3) Confidentiality of the communication is also included in almost all frameworks with sufficient attention.
4) Jamming-related risks are not considered by almost any framework.

5.7 Conclusion from the expert interviews

5.7.1 Answers to research questions for the expert interviews

Looking back, as an input to the interviews, we started with the following two statements:

a) **LoRaWan is risky**: 18 specific countermeasures exist that mitigate threats for technologies such as LoRaWan. In the design of the LoRaWan protocol version 1.0.2 class A, 10 out of those 18 countermeasures are not considered. For the remaining 8 that are considered, at least 5 are not designed well and are vulnerable.
b) **Frameworks do not address all risks**: The existing IOT frameworks from the industries cover 7 out of the 18 known countermeasures, and therefore only mitigate part of the threats. The remaining 11 are not covered in the frameworks.

To provide context to these statements a qualitative study was conducted in the form of expert interviews. The study addressed the following questions related to the statements.

1) **Root cause**: How do you explain the conclusions?
2) **Impact**: What impact does that have on consumers?
3) **Recommendation**: Should we do something about it and what?

During the interviews we answered these questions and learnt the following:

With regards to conclusion (a) LoRaWan is risky:

Root cause: It is not a problem that not all 18 specific countermeasures that mitigate threats are considered in the design of the LoRaWan protocol 1.0.2 class A, this was design choice. There is a need in the market also for protocols that offer out-of-the-box less security, but can be very useful for low power and long range communication devices and use cases where security is less of a concern. LoRaWan is one of them.

Impact: Each individual threat or vulnerability can have a high impact on consumers if LoRaWan is used in a specific use case that is directly affected by the threat or vulnerability. LoRaWan should not be used for use cases where security is relevant, such as payments, medical products, or safety related products. There are products on the market that do not respect this and risks are passed on to consumers without them being sufficiently aware. Whether the threats and vulnerabilities represent a cyber security risk for the consumer depends on the use case that a manufacturer implements using LoRaWan.

Attacks are either currently not yet happening, or are not detected. This could be attributed to a lack of use of the protocol to date, lack of monitoring on the side of network operators and solution providers, as well as lack of return on investments for the criminals at this moment.

Recommendations: Stakeholders agreed that LoRaWan should not be used for IOT consumer devices which require high level of security, because it is difficult to design a solution that is secure over this technology. That is the responsibility of IOT consumer product manufacturers.

With regards to conclusion (b) Frameworks do not address all risks:

Root cause: Frameworks are known to be of a poor quality, this is due to lack of incentives in the industry to create, publish and maintain good frameworks. Combined with the specifics of each solution, creating a generally applicable framework of a good quality is very hard.

Impact: A gap between the industry framework and academic research is a known fact that is not considered to be a problem by the interviewed experts.

Recommendations: The most important gap is a lack of openness both from the protocol manufacturers about how the protocol works, for which use cases it is recommended, what are the known threats that affect the protocol, what are the known vulnerabilities in the protocol design, and what should the implementers of the protocol and manufacturers of IOT devices take care of and how. This would address the knowledge gap better than frameworks.

5.7.2 Four principles for manufacturers

The interviews gave rise to the following 4 principles that should be considered by manufacturers whenever adopting LoRaWan:

Principle A) **Do not try to mitigate all risks**. LoRaWan is a risky protocol which does not mitigate many security risks. These are not expected to be mitigated in IOT solutions but rather avoided by using LoRaWan only in certain use cases.

Principle B) **Use LoRaWan only for products where security is not a concern**: Do not use LoRaWan as a technology in solutions where higher level of security is necessary and the existing threats are not mitigated by other means.

Principle C) **Be open about the use cases for which the product is developed**. Describe well the security design criteria with which the product was developed, and is expected to be used on the market. Describe which risks are mitigated and which are passed on to the consumer.

Principle D) **Do not rely on frameworks but rather conduct a custom risk assessment**. In case that a custom risk assessment is above your capability, an involvement of a specialist security expertise is desired.

5.7.3 Attention points for relevant stakeholder groups

The interviews also gave rise to the following key attention points for stakeholder groups involved in the LoRaWan ecosystem.

- **LoRaWan Alliance** (the protocol designers): increase the visibility and transparency around the protocol and its security posture. The biggest weakness the experts identified a lack of openness from the about the design and security of the LoRaWan protocol, which in combination with inevitably a lack of security knowledge on the endpoint device manufacturers will lead to usage of the protocol for use cases where it was not meant for, leading to risks to consumers. At least one example was identified where this has already happened.
- **Manufacturer of LoRaWan connected IOT consumer devices**: adopt the Principles A-D stated above.
- **Security Experts:** be reasonable when risk assessing solutions, and provide workable solutions that are acceptable and cost-effective.
- **Academia:** Participate more in the public and political, regulatory debate. Promote results among general public.
- **Consumers and awareness campaigners:** Increase knowledge of basic security awareness among consumers. Understand that LoRaWan is only meant for products where security is not of a concern.

6 Synthesis and Discussion

6.1 Revisiting the process

This thesis consists of a series of steps and conclusions.

We first limited the research to network and cybersecurity-related aspects of the connected consumer-grade IOT devices when using LoRaWan protocol 1.0.2 class A.

Then we conducted a desktop research and identified relevant threats, vulnerabilities, and mitigating measures by looking at industry frameworks and academic research. We looked at which of those counter-measures are implemented in the LoRaWan protocol version 1.0.2 class A. We derived two statements: (a) LoRaWan is risky and (b) Frameworks do not address all risks.

To provide context to these statements, a qualitative study was conducted in the form of expert interviews. We asked what is the root cause, and impact of the gaps and what can be done about it? Stakeholder interviews not only answered these questions but also gave rise to 4 principles for manufacturers of IOT devices, and attention points for other stakeholder groups.

See Figure 7 that depicts the line of research.

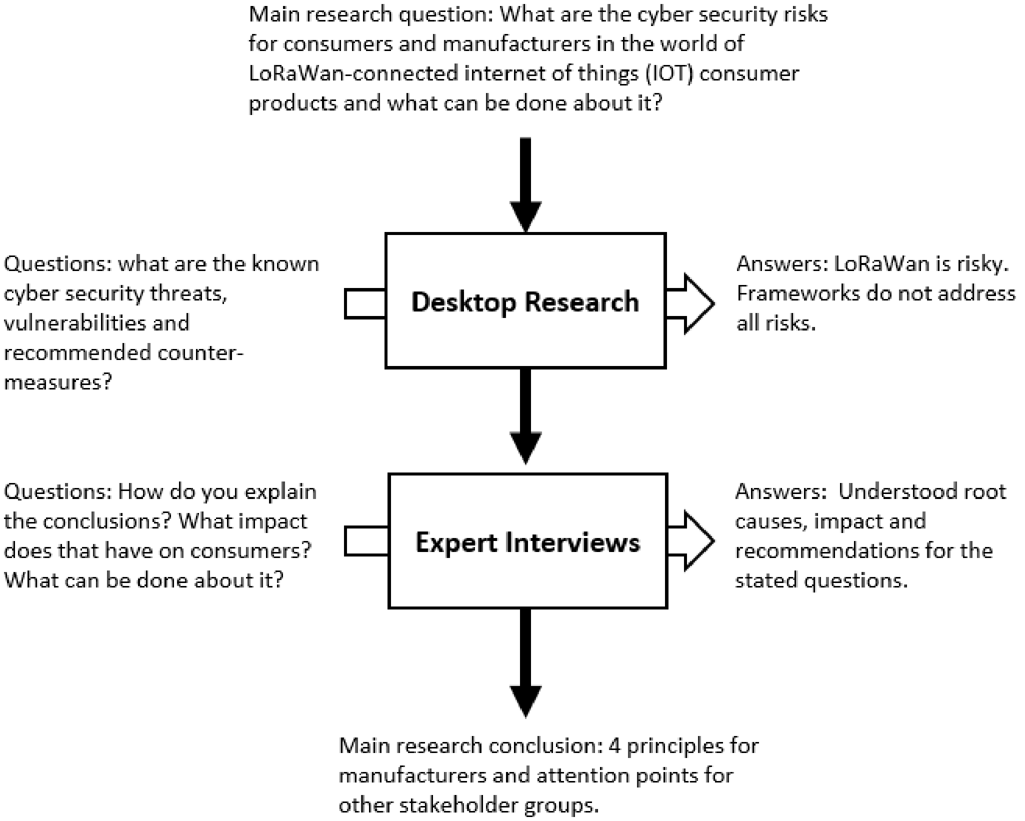
Main research question: What are the cyber security risks for consumers and manufacturers in the world of LoRaWan-connected internet of things (IOT) consumer products and what can be done about it?
Questions: what are the known cyber security threats, vulnerabilities and recommended counter-measures?
Desktop Research
Answers: LoRaWan is risky. Frameworks do not address all risks.
Questions: How do you explain the conclusions? What impact does that have on consumers? What can be done about it?
Expert Interviews
Answers: Understood root causes, impact and recommendations for the stated questions.
Main research conclusion: 4 principles for manufacturers and attention points for other stakeholder groups.

Figure 7: Figure depicting the flow of the research with the main questions asked and answerers provided. The bold arrow demonstrates the main line of research and the hollow around connection between sub-questions and sub-answers.

6.2 Revisiting the main research question

Revisiting the research problem: What are the cyber security risks for consumers and manufacturers in the world of LoRaWan-connected internet of things (IOT) consumer products and what can be done about it? We state the following answers.

What are the cyber security risks?

As part of the desktop research this thesis provided a comprehensive list of threats, vulnerabilities and mitigating measures that can be considered by manufacturers, network operators, and in the future improvements of the protocol. Such a comprehensive overview has not been to-date published.

Many threats and vulnerabilities are not mitigated in the LoRaWan version 1.0.2 class A protocol. Some are very practical, other rather academic. They should be taken into consideration by each manufacturer and consumer when designing and/or buying an IOT product. LoRaWan itself is vulnerable due to the fact that not all countermeasures are implemented, and some implemented countermeasures have weaknesses. Whether the threats and vulnerabilities represent a cyber security risk for the consumer depends on the use case that a manufacturer implements using LoRaWan. Stakeholders agreed that LoRaWan should not be used for systems which require high level of security, because it is difficult to design a solution that is secure over this technology. Attacks are either currently not yet happening, or are not detected. This could be attributed to a lack of use of the protocol to date, lack of monitoring on the side of network operators and solution providers, as well as lack of return on investments for the criminals at this moment.

What can be done about it?

We stated the following 4 principles that should be considered by manufacturers whenever adopting LoRaWan in order to protect consumers from unacceptable risks:

Principle A	Do not try to mitigate all risks.
Principle B	Use LoRaWan only for products where security is not a concern.
Principle C	Be open about the use cases for which the product is developed.
Principle D	Do not rely on frameworks but rather conduct a custom risk assessment.

We also stated main attention points for the following relevant stakeholder groups:

- **LoRa Alliance:** Increase the visibility and transparency around the protocol and its security posture.
- **Manufacturer:** Adopt the Principles A-D above.
- **Security Experts:** Be reasonable when risk assessing solutions and providing advice.
- **Academia:** Participate more in the public and political, regulatory debate. Promote own results outside of academic spheres.
- **Consumers and awareness campaigners**: Increase knowledge of basic security awareness among consumers. Have consumers understand that LoRaWan is only meant for products where security is not of a concern.

6.3 Limitations of the research

As any research, a number of assumptions and limitations apply to this research that should be taken when interpreting the results.

In Phase 1 (Desktop research), we took for granted a number of starting points.

Firstly, the list of known IOT frameworks [31] was used. This list was not approved by the academia, and does not claim to be a complete list, nor a list created using a strong methodology. Based on this list we derived the list of threats and countermeasures known to the industry. If certain frameworks were left aside different intermediate results could arise. However, the expert interviews confirmed a low quality of the available frameworks, and put less importance on those results.

Secondly a known list of countermeasures published in academia that are applicable to LPWAN protocols were used to evaluate which countermeasures are implemented in the LoRaWan protocol. This is not the only list of countermeasures ever published and it is possible that if the research started from another angle, a different intermediate would have been reached. However, the conclusions reached from the interview could be applied to any set of threats and countermeasures for LoRaWan, therefore this limitation should not severely impact the applicability of the results.

In Phase 2 (expert interviews), due to obvious limitations only a number of experts could have been approached for the interviews. A representative of a consumer, a device manufacturer, a network operator, a policy maker, an academia representative, and a managing consultant was selected. Other groups, notably chipset manufacturers, firmware manufacturers, journalists were not interviewed. All experts live and work in the Netherlands. The largest represented stakeholder group were management consultants who have a specific (often simplistic) view of the problems. This all could have contributed to a bias in the conclusions.

Overall, the scope of the research was limited to LoRaWan protocol version 1.0.2, class A. Classes B and C were not assessed to keep the research limited. At the same time as the research was ongoing, version 1.1 of LoRaWan was published where some of the known vulnerabilities are mitigated by newly implemented countermeasures. This could somewhat change the intermediate results, but will not affect the overall level of security built into the protocol. It will take months before LoRaWan 1.1. is supported by chipset manufacturers, endpoint devices and network operators, or even years before LoRaWan 1.0 is phased out of the market. Therefore the results in this document will for long be applicable.

6.4 Next steps

A lot of questions remain unanswered and are subject for further study.

This thesis looked at the use of LoRaWan 1.0.2 class A in consumer products. An obvious question arise: how about industrial IOT devices, would the risks and their perception change if LoRaWan was deployed in industrial control systems or SCADA environments?

Classes B and C of the protocol were not studied.

LoRaWan protocol version 1.1 was recently released and came with improvements, some of which are related to security. This leaves room for additional study of vulnerabilities and countermeasures for those aspects.

Privacy aspects were mostly left out of scope for this thesis.

A lot more could have been said about regulation of IOT. All participants in the research agreed that regulation could solve a lot of the burning issues, but no clear agreement was reached about the form such regulation should take. This would require a more thorough research.

All these topics introduce an opportunity for further research.

7 List of tables and figures

Table 1: Interview Guide 18
Table 2: List of experts who participated in the interviews 19
Table 3: Coding Manual 20
Table 4: Existing IOT check-lists (guidelines and frameworks) considered as input to the research 21
Table 5: LoRaWan specific Vulnerabilities and Countermeasures 40
Table 6: Comparison of Practice and Theory for recommended countermeasures 41

Figure 1: Focus of the research in context of the IOT ecosystem. 5
Figure 2: Model for IOT security architecture with the focus area highlighted 11
Figure 3: High level process 12
Figure 4: Core part of the process for consolidating known and relevant threats and mitigating measures. 13
Figure 5: High level process for expert interviews 15
Figure 6: Specific LoRaWan Ecosystem Stakeholders used as a model for selecting experts and scheduling interviews. 17
Figure 7: Figure depicting the flow of the research with the main questions asked and answerers provided. The bold arrow demonstrates the main line of research and the hollow around connection between sub-questions and sub-answers. 60

8 Works Cited

[1] K. Ashton, "That 'Internet of Things' Thing," RFID Journal, 22 June 2009. [Online]. Available: http://www.rfidjournal.com/articles/view?4986. [Accessed 1 November 2017].

[2] Networked Enterprise & RFID & Micro & Nanosystems, "Roadmap for the Future," in *Co-operation with the Working Group RFID of the ETP EPOSS, Internet of Things in 2020*, 2008.

[3] R. Dijkmana, B. Sprenkelsa, T. Peetersa and A. Janssen, "Business models for the Internet of Things," *International Journal of Information Management,* no. 35, pp. 672-678, 2015.

[4] IEEE Internet Technology Policy Community White Paper, "Internet of things (IOT) security best practices," IEEE, 2017.

[5] L. Srivastava, "Pervasive, ambient, ubiquitous: the magic of radio," in *Proceedings of uropean Commission Conference ''From RFID to the Internet of Things"*, Bruxelles, 2006.

[6] H. Sundmaeker, P. Guillemin, P. Friess and P. Woelfflé, Vision and Challenges for Realising the Internet of Things, Brussels: European Commission - Information Society and Media DG, 2010.

[7] A. Kusiak, "Smart Manufacturing," *International Journal of Production Research,* 2017.

[8] Gartner, "Internet of Things (IoT) Security Market Worth 29.02 Billion USD by 2022," Gartner, 2017.

[9] "Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Critical Infrastructure Protection in the fight against terrorism," 2010.

[10] Deloitte, "Smar Cities: How rapid advances in technology are reshaping our economy and society," Deloitte, 2015.

[11] "Internet of Things in Smart Cities Market –Global Forecast to 2020," Markets & markets, [Online]. Available: http://www.marketsandmarkets.com.

[12] M. Walker, "Hype Cycle for Emerging Technologies," Gartner, 2017.

[13] Reuters, "Uber suspends self-driving car program after Arizona crash," [Online]. Available: https://www.cnbc.com/2017/03/26/uber-self-driving-car-arizona-crash-suspended.html. [Accessed 17 November 2017].

[14] Wired, "Tesla Bears Some Blame for Self-Driving Crash Death, Feds Say," [Online]. Available: https://www.wired.com/story/tesla-ntsb-autopilot-crash-death/. [Accessed 15 November 2017].

[15] Bundesamt fur Sicherheit in der Informationstechnik, "Die Lage der IT-Sicherheit in Deutschland 2014," 2014.

[16] A. Greenberg, "Hackers remotely kill a jeep on the highway—with me in it," Wired, [Online]. Available: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Accessed 10 October 2017].

[17] A. Chapman, "Hacking into internet connected light bulbs," Contextis, [Online]. Available: http://contextis.com/resources/blog/hacking-internet-connected-light-bulbs. [Accessed 12 November 2017].

[18] "IOT Design Manifesto 1.0," May 2015. [Online]. Available: https://www.iotmanifesto.com/. [Accessed 17 November 2017].

[19] N. Woolf, "DDoS attack that disrupted internet was largest of its kind in history, experts say," The Guardian, 26 October 2016. [Online]. Available: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[20] S. Spary, "Online Criminals Are Targeting Fitbit User Accounts," BuzzFeed News, 6 January 2016. [Online]. Available: https://www.buzzfeed.com/saraspary/online-criminals-are-targeting-fitbit-user-accounts?utm_term=.xlEZ51e6aA#.inXMpLvJzw.

[21] L. Cai and H. Chen, "Touchlogger: Inferring keystrokes on touch," *Hotsec,* 2011.

[22] Z. Xu, K. Bai and S. Zhu, "Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors," in *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*.

[23] W. Chen, G. Xiaonan , W. Yan and C. Yingying, "Friend or Foe?: Your Wearable Devices Reveal Your Personal PIN," in *AsiaCCS 2016*, Xi'an, 2016.

[24] "LoRa Alliance Technology: Wide Area Network for IOT," [Online]. Available: https://www.lora-alliance.org/technology. [Accessed 2016 June 39].

[25] KPN, "The Netherlands has first nationwide LoRa network for Internet of Things," [Online]. Available: https://corporate.kpn.com/press/press-releases/the-netherlands-has-first-nationwide-lora-network-for-internet-of-things-.htm. [Accessed 2017 June 30].

[26] GEOWAN, "Cattle Tracking GEOWAN," [Online]. Available: http://www.geowan.net/cattle-tracking/. [Accessed 29 November 2017].

[27] Dimo Systems B.V., "xignal Mousetrap," [Online]. Available: https://www.xignal.com/products/xignal-mousetrap. [Accessed 30 November 2017].

[28] M. O'Neill, "Insecurity by Design: TOday's IoT Device Security Problem," *Engineering 2,* pp. 48-49, 2016.

[29] P. P. Ray, "A survey on Internet of Things architectures," *Journal of King Saud University - Computer and Information Sciences,* 2016.

[30] M. Abomhara and G. Koien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *Journal of Cyber Security,* vol. 4, pp. 65-88, 2015.

[31] B. Schneiner, "Security and Privacy Guidelines for the Internet of Things," Schneier on Security, [Online]. Available: https://www.schneier.com/blog/archives/2017/02/security_and_pr.html. [Accessed 2017 November 5].

[32] A Broadband Internet Technical Advisory Group, "Internet of Things (IoT) Security and Privacy Recommendations," 2016. [Online]. Available: http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf. [Accessed 2017 September 28].

[33] OWASP, "IoT Security Guidance," [Online]. Available: https://www.owasp.org/index.php/IoT_Security_Guidance. [Accessed 24 November 2017].

[34] U.S. Department of Homeland Security, "Strategic Principles for Security the Internet of Things (IOT)," 2016. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf. [Accessed 2017 September 24].

[35] OneM2M, "Technical report Security," 2016. [Online]. Available: http://www.onem2m.org/images/files/deliverables/Release2/TR-0008-Security-V2_0_0.pdf. [Accessed 2017 October 01].

[36] OneM2M, "Technical report Security Solutions," 2016. [Online]. Available: http://onem2m.org/images/files/deliverables/Release2/TS-0003_Security_Solutions-v2_4_1.pdf. [Accessed 1 October 2017].

[37] GSM Association, "IoT Security Guidelines Overview Document," [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.11-v1.1.pdf. [Accessed 10 October 2017].

[38] GSM Association, "IoT Security Guidelines for Service Ecosystems," [Online]. Available: http://www.gsma.com/connectedliving/wp-content/uploads/2016/02/CLP.12-v1.0.pdf. [Accessed 10 October 2017].

[39] GSM Association, "IoT Security Guidelines for Endpoint Ecosystems," [Online]. Available: http://www.gsma.com/connectedliving/wp-content/uploads/2016/02/CLP.13-v1.0.pdf. [Accessed 10 October 2017].

[40] GSM Association, "IoT Security Guidelines for Network Operators," [Online]. Available: http://www.gsma.com/connectedliving/wp-content/uploads/2016/02/CLP.14-v1.0.pdf. [Accessed 10 October 2017].

[41] Internet of Things Security Foundation, "Establishing Principles for Internet of Things Security," [Online]. Available: https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf. [Accessed 10 October 2017].

[42] Afdeling Buitengewone Zaken, Beyond.io, FROLIC Studio, The Incredible Machine, "IOT Design Manifesto," [Online]. Available: https://www.iotmanifesto.com/wp-content/themes/Manifesto/Manifesto.pdf. [Accessed 10 October 2017].

[43] City of New York, "NYC Guidelines for the Internet of Things," [Online]. Available: https://iot.cityofnewyork.us/. [Accessed 10 October 2017].

[44] IoT Security Foundation, "IoT Security Compliance Framework," [Online]. Available: https://iotsecurityfoundation.org/wp-content/uploads/2016/12/IoT-Security-Compliance-Framework.pdf. [Accessed 24 October 2017].

[45] Cloud Security Alliance, IoT Working Group, "Future-proofing the Connected World," [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf. [Accessed 10 November 2017].

[46] Online Trust Alliance, "IoT Security & Privacy Trust Framework," [Online]. Available: http://otalliance.actonsoftware.com/acton/attachment/6361/f-008d/1/-/-/-/-/IoT%20Trust%20Framework.pdf. [Accessed 10 November 2017].

[47] I Am The Cavalry, "Five Star Automotive Cyber Safety Framework," [Online]. Available: https://www.iamthecavalry.org/wp-content/uploads/2014/08/Five-Star-Automotive-Cyber-Safety-February-2015.pdf. [Accessed 10 November 2017].

[48] I Am The Cavalry, "Hippocratic Oath for Connected Medical Devices," [Online]. Available: https://www.iamthecavalry.org/wp-content/uploads/2016/01/I-Am-The-Cavalry-Hippocratic-Oath-for-Connected-Medical-Devices.pdf. [Accessed 10 November 2017].

[49] Industrial Internet Consortium Security Working Group, "Industrial Internet of Things Volume G4: Security Framework," [Online]. Available: http://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf. [Accessed 10 November 2017].

[50] A. Tanenbaum and D. Wetherall , Computer Networks fifth edition, Pearson Education, 2010.

[51] (ISC)2, Official (ISC)2 Guide to the CISSP CBK Third Ed., Taylor & Francis Ltd , 2012.

[52] Franklin Heath Ltd, "LPWA Technology Security Comparison," Franklin Heath Ltd, 2017.

[53] N. Sornin, M. Luis, T. Eirich, T. Kramp and O. Hersent, "LoRaWAN™ Specification v. 1.0.2," LoRa Alliance, 2016.

[54] S. Tomasin, S. Zulian and L. Vangelista, "Security Analysis of LoRaWAN Join Procedure for Internet of Things Networks," in *IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, San Francisco, CA, USA, 2017.

[55] X. Yang, "LoRaWAN: Vulnerability Analysis and Practical Exploitation," Delft University of Technology, Delft, the Netherlands, 2017.

[56] M. Labib, S. Ha and W. Saad, "A Colonel Blotto Game for Anti-Jamming in the Internet of Things," in *Global Communications Conference (GLOBECOM)*, San Diego, CA, USA, 2015.

[57] B. Reynders, W. Meert and S. Pollin, "Range and coexistence analysis of long range unlicensed communication," in *23rd International Conference on Telecommunications (ICT)*, Thessaloniki, Greece, 2016.

[58] E. Aras, G. S. Ramachandran and P. Lawrence, "Exploring the Security Vulnerabilities of LoRa," in *3rd IEEE International Conference on Cybernetics (CYBCONF)*, Exeter, UK, 2017.

[59] Y.-C. Hu, A. Perrig and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *22nd Annual Joint Conference of the IEEE Computer and Communications*, San Francisco, CA, USA, 2003.

[60] M. van Leent, "An improved key distribution and updating mechanism for low power wide area networks (LPWAN)," Cyber Security Academy, 2017.

[61] S. Naoui , M. E. Elhdhili and L. A. Saidane, "Enhancing the security of the IoT LoraWAN architecture," in *International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)*, Paris, France, 2016.

[62] P. Girard, "Low Power Wide Area Security," Gemalto, 2015.

[63] J. Lee , D. Hwang and D. Park, "Risk analysis and countermeasure for bit-flipping attack in LoRaWAN," in *International Conference on Information Networking (ICOIN)*, Da Nang, Vietnam, 2017.

[64] K. Paterson, and A. Yau, "Cryptography in Theory and Practice: The Case of Encryption in IPsec," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2006.

[65] R. Miller, "LoRa Security, Building a Secure LoRa Solution," MWR Labs Whitepaper.