Lappeenranta University of Technology
School of Business and Management
Degree Program in Computer Science

Jouni Pänkäläinen

INFORMATION SECURITY IN THE INTERNET OF THINGS – A SYSTEMATIC LITERATURE REVIEW

Examiners : Professor Jari Porras
DSc Antti Knutas

Supervisors: Professor Jari Porras

ABSTRACT

Lappeenranta University of Technology
School of Business and Management
Degree Program in Computer Science

Jouni Pänkäläinen

Information security in the Internet of Things – a systematic literature review

Master's Thesis

2016

76 pages, 5 figures, 7 tables, 1 appendix

Examiners: Professor Jari Porras
DSc Antti Knutas

Keywords: Internet of Things, security

In this thesis a systematic literature review about the security in the Internet of Things was performed. Based on the chosen search strategy, 38 articles were selected for a closer examination. Out of these articles, the concerns and solutions for the security in the Internet of Things were extracted. The security in the Internet of Things is under heavy research. Most of the research has been done in the recent years. IoT devices often collect private information and the vast number of the devices allow them to be exploited in malicious attacks. Many difficult problems, such as privacy and authentication still require efficient solutions for the heterogeneous and resource constrained environment of the IoT. However, the research for the means to achieve secure communication in the IoT is ongoing and many promising solutions are already emerging.

TIIVISTELMÄ

Lappeenrannan teknillinen yliopisto
School of Business and Management
Tietotekniikan koulutusohjelma

Jouni Pänkäläinen

Tietoturva asioiden Internetissä – systeemaattinen kirjallisuuskatsaus

Diplomityö

2016

76 sivua, 5 kuvaa, 7 taulukkoa, 1 liite

Työn tarkastajat: Professori Jari Porras
TkT Antti Knutas

Hakusanat: asioiden Internet, tietoturva

Tässä työssä suoritettiin systemaattinen kirjallisuuskatsaus tietoturvasta asioiden Internetistä. Valittujen hakukriteerien perusteella 38 artikkelia valittiin lähempään tarkasteluun. Näistä artikkeleista poimittiin sekä huolet tietoturvasta asioiden Internetissä, että mahdolliset ratkaisut näihin huoliin. Tietoturvaa asioiden Internetissä tutkitaan ahkerasti. Suurin osa tutkimuksista on julkaistu lähivuosina. Laitteet asioiden Internetissä keräävät paljon yksityistä tietoa ja laitteiden suuri määrä mahdollistaa niiden käytön pahantahtoisiin tarkoituksiin. Monet vaikeat ongelmat, kuten yksityisyydensuoja ja laitteiden tunnistautuminen vaativat vielä tehokkaita ratkaisuja asioiden Internetin moninaiseen ja resurssiköyhään ympäristöön. Aiheen tutkimus on kuitenkin tuottanut jo monia lupaavia tuloksia.

ACKNOWLEDGEMENTS

This thesis is the culmination of nine years' worth of experience. I'd like to thank my friends graduating before me and giving me motivation to finish my own studies. I'd also like to thank the teachers and faculty members of the Lappeenranta University of Technology for bearing with me through all of these years. Special thanks to Cluster ry for giving me a bunch of lifelong friends and delaying my studies for a good few years.

TABLE OF CONTENTS

LIST OF SYMBOLS AND ABBREVIATIONS

2-ACKT	Two-Way Acknowledgement-Based Trust
AMQP	Advanced Message Queuing Protocol
API	Application Program Interface
BeTaaS	Building the environment for the Things as a Service
BLE	Bluetooth Low Energy
CoAP	Constrained Application Protocol
CLT	Collaborative Lightweight Trust-based Routing Protocol
DDS	Data Distribution Service
DDoS	Distributed Denial of Service
DODAG	Destination Oriented Directed Acyclic Graph
DoS	Denial of Service
DNS	Domain Name System
DNS-SD	DNS Service Discovery
DTLS	Datagram Transport Layer Security
FTC	Federal Trade Commission
GTMS	Group-Based Trust Management Scheme
HAN	Home Automation Network
HTTP	Hypertext Transfer Protocol
IoT	Internet of Things
IoT-A	Internet of Things Architecture
IoV	Internet of Vehicles
IoT@Work	Internet of Things at Work
IP	Internet Protocol
IPSec	Internet Protocol Security
LA	Learning Automata
LTE- A	Long Term Evolution – Advanced
M2M	Machine-to-machine
MAC	Medium Access Control
mDNS	Multicast DNS

MTC	Machine-Type Communications
MTU	Maximum Transmission Unit
MQTT	Message Queue Telemetry Transport
NFC	Near Field Communication
OLP	Object Level Protection
OpenIoT	Open source cloud solution for the Internet of Things
REST	REpresentational State Transfer
RPL	Routing Protocol for Low Power and Lossy Networks
SHAS	Smart Home Automation System
SMRP	Secure Multi-Hop Routing Protocol
TaaS	4Things as a Service
TSFR	Trust-Aware Secure Routing Framework in Wireless Sensor Networks
TLS	Transport Layer Security
UPECSI	User-driven Privacy Enforcement for Cloud-based Services in the IoT
WPAN	Wireless Personal Area Network
XMPP	Extensible Messaging and Presence Protocol

1 INTRODUCTION

The modern idea of the Internet of Things was first introduced by Mark Weiser in 1991 [1]. Weiser wrote “The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.”. In his article, Weiser talked about interconnected devices that disappear to the background of our everyday lives.

A little more than a decade later, his futuristic vision is becoming a reality. Since the start of 21st century, the Internet has spread everywhere. Gartner [2] has estimated, that 6.4 billion devices will be connected to the Internet in 2016. This is 30 percent more than in 2015. A growing number of these devices are so called Internet of Things (IoT) devices.

Global Standards Initiative defines [3] the Internet of Things as “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies”. This means that beside the traditional Internet “things”, such as desktop and laptop computers, the IoT definition contains such things as cars, clothing and even buildings. With all these devices necessary for everyday life connected to the Internet, comes all new security concerns. No longer is it enough to secure the doors and windows of your apartment, you also have to think about the information security of your fridge or thermostat.

There has been some previous research done on the subject. In 2014 Kumar et. al. [4] performed a survey on security and privacy issues of the Internet of Things. They identified multiple security concerns in all areas of the IoT: front-end systems, networks and back-end systems. In addition, many privacy concerns were identified. The privacy in devices, communications, storage solutions, and at the data processing phase were all questioned.

In 2013 Zhao et al. [5] surveyed the security in the Internet of Things. They identified problems on all layers of the IoT model. Perception layer contained the most problems. The problems ranged from node capture to routing and timing attacks. Network layer contained traditional security security problems, but also privacy and compatibility problems. Application layer security problems included data access permissions, data protection and software vulnerabilities. They also offered some possible solutions to these problems.

Suo et. al. [6] also review the security in the IoT. They examined security requirements and problems in the different layers of the IoT. They found that main problems are encryption, communication security, protecting sensor data, and cryptographic algorithms.

There are also many reviews, which do not directly handle security, but still mention it in some way. In 2013 Perera et. al. surveyed Context Aware Computing for the IoT. They state "Security and privacy issues in context-aware computing are not researched and seriously considered in many solutions." In 2010 Atzori et. al. [7] performed an extensive survey on IoT. They mention vulnerable devices, authentication and data integrity, man-in-the-middle attacks. They also mention privacy problems such as unwanted data collection.

In 2015 Li et. al [8] also performed a survey on the IoT. They state "The existing network security technologies can provide a basis for privacy and security in IoT, but more work still need to be done". In addition, they mention that two aspects still require further study: 1) The adaptation of existing Internet standards for interoperable protocols and 2) the security assurance for composable services.

Even with this research, the research in the IoT security is still rapidly ongoing. This research attempts to both collect the results of the previous research and see if any new problems have arisen and if there are solutions found for the existing problems.

1.1 Goals and delimitations

The goal of this thesis is to find out the current state of the information security research regarding the Internet of Things. This thesis will attempt to answer the following research questions.

- RQ1: When and how was this research published?
- RQ2: Which application domains have been researched?
- RQ3: What kinds of security concerns have been raised about the Internet of Things?
    - RQ3.1 Do different application domains have specific security concerns?
- RQ4: What kinds of solutions have been presented for improving the security of the Internet of Things?
    - RQ4.1: What kinds of application domain specific information security solutions have been presented?
- RQ5: Does the current research have any significant gaps?

These questions will be answered using a systematic literature review [9] of the subject matter, in order to remove any selection bias. This thesis will only focus on the security and usability of the Internet of Things in general. No specific algorithms or technologies are examined, only the general concepts affecting the security in the IoT.

1.2 Structure of the thesis

Chapter 2 of this thesis gives an overview on the concepts in the IoT and security required to understand the rest of the thesis. Chapter 3 of this thesis defines the search strategy and search terms used. Chapter 4 discusses the results for each specific research question. In chapter 5 discussion and conclusions are presented. Chapter 6 summarizes the rest of the thesis.

2 BACKGROUND

In this chapter, background information about information security and the Internet of Things is introduced. The concepts of information security are described very superficially, while the Internet of Things is given a bit more in-depth look.

2.1 Information Security

In order to achieve a secure Internet of things, the following security features and properties have been defined [10] and must be considered when building an IoT network:

- **Availability:** All nodes must be able to access services at every layer even in the presence of malicious attacks.
- **Authenticity:** Nodes must identify and prove their identity in the network.
- **Confidentiality:** Information can't be seen by the wrong sources
- **Integrity:** Information can't change while it's in transit
- **Non-repudiation:** All network nodes can't deny knowledge of the data that they've sent or received in order to identify untrusted nodes sending false data or silently receiving confidential data

These basic principles are achieved by utilizing security requirements, security policies and security mechanisms [11]. The security requirements specify what needs to be protected. For example, a company needs to protect the integrity of its customer data, but it must also keep its services available online. Requirements determine what actions are allowed and what actions are disallowed. These actions then form the security policy. In case of the aforementioned company, its policy might dictate that employees are allowed to access customer data, but nobody outside the company is allowed access to that data. When all of the policies are met, the system is secure. If anyone can perform a disallowed action, the system is nonsecure.

Security policies are enforced by security mechanisms. The mechanisms may be technical or operational. Technical mechanisms are things such as an access control system, which determines who is allowed to access what data in a system. Technical mechanisms are not

suitable for all policies. For example, the example company may forbid employees the use of their own removable media devices, but technically this is not enforceable. Operational enforcement mechanism would be the threat to suspend any employee caught using their own removable media. The security mechanisms are not infallible. The question whether a set of security mechanisms correctly enforce a security policy is a depends on security assurances [11].

The security assurances measure how well mechanisms enforce policies. There are many different methodologies for elevating the assurances. The methodologies may be structured as a part of the software development process. No methodology can guarantee an absolute assurance that the system is safe, but they usually improve its security noticeably [11].

2.2 Internet of things

The Internet of Things is a communication paradigm in which objects of everyday life are able to communicate with each other in order to achieve common goals. These objects are often called “things” or “entities”. Enabling this small scale inter-device communication, things such as smart homes and smart cities can be built [7]. In this chapter the common structure and terms of the IoT and some of the protocols used in the IoT are introduced.

2.2.1 The layered approach

Like traditional networking, the Internet of Things is divided into layers. However, the layer model is not yet standardized [12]. Depending on the author, there are either three [13,14,5], four [15], or even more [12] layers as seen on Figure 1. The common layers are application layer, network layer and physical layer. The common layers for both models are application layer, network layer and physical layer. The four-layer model adds the perception layer in between application and network layer.

Application layer hosts the services and applications running on top of the IoT. The IoT applications involve things such as smart cities and smart homes. The business layer manages the overall IoT system activities and has the ability to build business models,

graphs and flowcharts based on the data received from the application layer. The service management layer is also known as Middleware. The service management layer allows programmers to work on abstract objects instead of worrying about the underlying hardware [12].

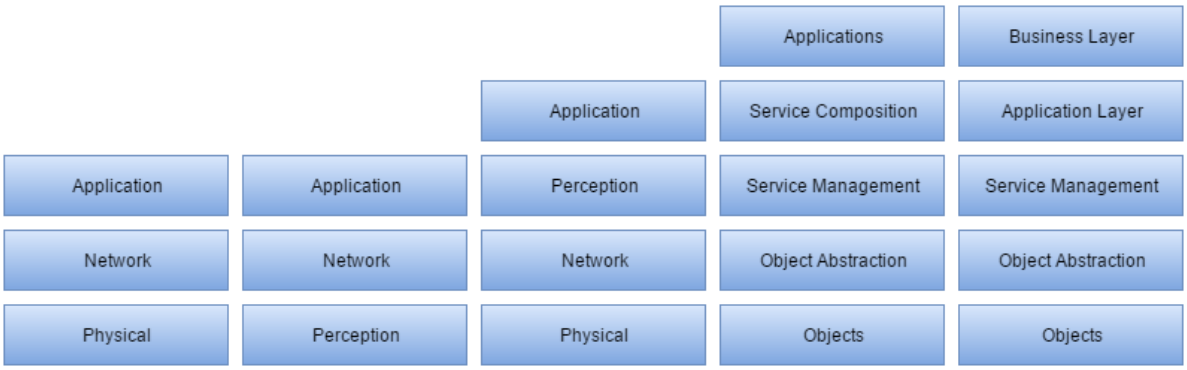

Figure 1. The many layer models of IoT. (References from left to right [13], [14], [15], [12], [12])

The perception layer includes the sensory technologies that give the IoT devices the ability to sense the environment around them. Perception layer includes technologies like temperature sensors and RFID chips. In the three-layer model the perception layer is included within the network layer [13]. The object abstraction layer is equivalent to the perception layer. The network layer handles the network communications for the IoT. This layer includes things as servers and network nodes and components. Finally, the physical or the objects layer contains the actual devices that act as the backbone for the IoT [15,12].

2.2.2 The elements of Internet of Things

To understand the Internet of things, one must understand how it's built. Figure 2 shows the elements of the Internet of Things. These elements represent the basic building blocks needed to deliver the functionality of IoT. Each of these has a specific functionality in the Internet of things [12].

Identification refers to how services are named within the IoT. It is used to differentiate between object's ID and its address. Separating object's identification and addressing is

important, since identification methods are not globally unique. Identification methods are used to provide an identity for each object within the network [12].

Figure 2. The elements of the Internet of Things [12]

Sensing means gathering data from related objects in the network and sending it forward for processing. The data can be gathered by smart hubs, that can monitor and control thousands of smart devices. The data is often produced by smart sensors connected to Single Board Computers, such as Arduino or Raspberry PI [12].

The IoT connects heterogeneous objects together. For this, multiple different communication technologies are needed. The IoT devices require usually low power consumption and high resilience to lossy and noisy communication links. These technologies can be for example Bluetooth, WiFi or Near Field Communication (NFC) [12].

The data gathered by the smart devices needs to be processed somehow. The data is processed by processing units such as microcontrollers and SOCs. These processing units use different kinds of real-time operating systems, such as Contiki. The computations can also be performed in cloud platforms [12].

The IoT services can be categorized under four classes: Identity-related services, Information Aggregation services, Collaborative-Aware services and Ubiquitous services. Identity-related services offer object identification to applications. Information Aggregation services collect and summarize the raw sensory data an offer it to applications. Collaborative-Aware services make decision based on the Information

Aggregation services' data. Ubiquitous services make Collaborative-Aware services available to anyone, anywhere at any time [12].

Semantics means that the IoT is able to extract knowledge from different machines to provide the right services at the right time. Knowledge extraction includes discovering and using resources, modeling information and recognizing and analyzing data. Semantics can be seen as the brain of IoT [12].

2.2.3 Protocols

Despite still being in its infancy, there are already many protocols and standards developed for the IoT. The IoT protocols can be divided into four different broad categories: application protocols, service discovery protocols, infrastructure protocols and other influential protocols [12]. These are summarized in Table 1. In this subchapter, the most common protocols are shortly introduced.

Table 1. Protocols of the IoT [12]

<table>
<tr><td colspan="2">Application protocols</td><td>DDS</td><td>CoAP</td><td>AMQP</td><td>MQTT</td><td>MQTT-SN</td><td>XMPP</td><td>HTTP REST</td></tr>
<tr><td colspan="2">Service discovery</td><td colspan="4">mDNS</td><td colspan="3">DNS-SD</td></tr>
<tr><td rowspan="4">Infrastructure protocols</td><td>Routing protocol</td><td colspan="7">RPL</td></tr>
<tr><td>Network Layer</td><td colspan="4">6LoWPAN</td><td colspan="3">IPv4/IPv6</td></tr>
<tr><td>Link Layer</td><td colspan="7">IEEE 802.15.4</td></tr>
<tr><td>Physical/Device Layer</td><td colspan="2">LTE-A</td><td colspan="2">EPCglobal</td><td colspan="2">IEEE 802.15.4</td><td>Z-Wave</td></tr>
<tr><td colspan="2">Influential protocols</td><td colspan="4">IEEE 1888.3, IPSec</td><td colspan="3">IEEE 1905.1</td></tr>
</table>

2.2.3.1 Application protocols

Constrained Application Protocol (CoAP) defines a web transfer protocol for IoT devices based on REpresentational State Transfer (REST). REST represents a way to exchanged data between clients and servers over HTTP. Unlike REST, CoAP is transferred over UDP

(instead of TCP) by default. This makes it more suitable for IoT applications. CoAP also modifies some of the HTTP functions to conform to low power consumption requirements and to enable operation over lossy and noisy links. Since CoAP is based on REST, the conversion between the two protocols can be done over REST-CoAP proxies [12].

Message Queue Telemetry Transport (MQTT) connects embedded devices and networks with applications and middleware. MQTT uses the publish/subscribe pattern in order to provide flexibility and simplicity to implementations. MQTT is a good fit for IoT, since it is suitable for resource constrained devices and works on slow and unreliable links. MQTT is built on top of TCP protocol. There also exists an UDP version of the MQTT called MQTT-SN, which was built specifically for sensor networks [12].

Extensible Messaging and Presence Protocol (XMPP) is a decentralized instant messaging standard, that allows users to communicate over the Internet regardless of the operating system they are using. Many of the XMPP features make it relevant to the scope of IoT. It's secure, platform independent, decentralized and also allows extensibility by adding new applications on top of the core protocols [12].

Advanced Message Queuing Protocol (AMQP) is an IoT protocol for message-oriented environments. It provides reliable communication via message delivery guarantee primitives such as at-most-once, at-least-once and exactly once. AQMP has two main components: exchanges and message queues. Exchanges route messages to appropriate queues and exchanges based on pre-defined rules. Queues are used to store the messages and then sent to receivers. AQMP also supports the publish/subscribe model [12].

Data Distribution Service (DDS) is a publish/subscribe protocol for real-time machine-to-machine (M2M) communications. Unlike MQTT or AQMP, DDS uses a broker-less architecture and uses multicasting. The broker-less publish/subscribe architecture suits well for real-time IoT and M2M communications [12].

2.2.3.2 Service discovery protocols

The IoT requires a mechanism that allows the dynamic discovery and registration of services and devices. For this, two protocols are mainly used: multicast DNS (mDNS) and DNS Service Discovery (DNS-SD). Both have been originally designed for resource rich devices, but there have been studies to adapt light-weight versions of them for IoT [12].

mDNS performs the task of a traditional unicast Domain Name System (DNS) server in a multicast manner. It inquires names by sending multicast query to all nodes in the local domain and asks that the devices contained in the query reply back. The devices with the given name then send a multicast message containing their IP address and all of the devices in the network, that receive the message, update their local cache using the name and the IP address.

DNS-SD utilizes mDNS to allow clients to discover services over the standard DNS. DNS-SD sends DNS packages to specific multicast addresses. DNS-SD finds the hostnames of the required services and pairs them with an IP address. First the DNS-SD sends a multicast query to ask for host names for specific services and the uses the mDNS to pair those services with addresses [12].

2.2.3.3 Infrastructure protocols

Routing Protocol for Low Power and Lossy Networks (RPL) was created to support minimal routing requirements over lossy links. It supports multipoint-to-point, point-to-multipoint and point-to-point traffic models. RPL utilizes a Destination Oriented Directed Acyclic Graph (DODAG) to represent the routing of the nodes. Each node in the graph is aware of their parents, but have no information about their children. Each node is also guaranteed to have a path to the root of the graph and a preferred parent for increased performance. The graph is formed when the root node starts sending its location to all network levels. Each child node registers the path to the parent and propagates this message forward [12].

6LoWPAN was created as an adaptation layer to fit IPv6 packages to the special characteristics of low power Wireless Personal Area Networks (WPAN). The protocol maps services required by the IPv6 over low power WPANs. It provides header compression to reduce overhead, fragmentation to meet the IPv6 Maximum Transmission Unit (MTU) requirement and forwarding to link-layer. 6LoWPAN removes a lot of IPv6 overhead and can compress IPv6 headers to two bytes [12].

IEEE 802.15.4 was created to specify a sub-layer for Medium Access Control (MAC) and a physical layer for low-rate WPANs. It is also used in the IoT to provide reliable communication and operability on different platforms. It can handle about 65 000 nodes and provides high level security, encryption and authentication services [12].

Bluetooth Low Energy (BLE) is a version of Bluetooth, that uses a low-power short range radio to operate much longer than previous versions. It's range coverage is about 100 meters and its latency is 15 times shorter than the classic Bluetooth. These features make it a great choice for IoT applications.
Long Term Evolution – Advanced (LTE-A) is a set of cellular communication protocols for Machine-Type Communications (MTC) and IoT infrastructures. It outperforms other cellular solutions in terms of cost and scalability. Its downside is high network congestion with large number of devices [12].

Z-Wave is a low-power wireless communication protocol for Home Automation Networks (HAN). It's meant for application that require tiny data transmission, such as light and appliance controllers. It has a range of 30 meters for point-to-point communication and a transmission rate of 40 kbps [12].

2.2.4 Discussion

The Internet of Things enables a wide array of new applications and offers new solutions to existing problems. However, the heterogeneous and open nature of the IoT present numerous problems for information security. The low computational power of the devices

shuts out many of the current cryptographic solutions. The node based architecture allows attackers to gain a physical access to the devices easier.

The most important elements to protect in the IoT are identification, communication and computation. Insecure identification allows attackers to insert malicious nodes into the network and thus cause problems. Insecure communication is easy to eavesdrop and even alter by malicious entities. Finally, insecure computation allows attackers to read and alter gathered data. The other elements can also be vulnerable to attackers, but the attacks are harder to perform. Altering the data gathered by sensors in the sensing phase is not always very easy and the services and semantics may be harder to alter to one’s liking than simply changing the raw data to get the desired result.

3 RESEARCH SETUP

The search was performed using the Systematic Literature Review (SLR) guidelines [9]. The SLR consists of the following steps:

1. Protocol preparation (research questions, process, etc.)
2. Doing an expert survey (consult experts for keywords and publications for pilot study)
3. Carrying out a pilot study
4. Conducting the actual research
5. Data extraction
6. Analysis of the reports
7. Development of conclusions
8. Reporting

3.1 Protocol preparation

The SLR research questions selected were the same as described in chapter 1.1. The articles with following properties were selected for further review:

- Published between 1.1.2006 and 31.7.2016
- Topic is about the Internet of Things
- Topic is about information security
- Scientific and peer reviewed articles
- Relevant to the research question

Information security is a vast field of research. In order to keep the amount of articles reasonable, the following exclusion criteria was selected:

- Articles concerning specific technologies, such as protocols or identity management methods
- Articles concerning a specific part of the IoT and not IoT as a whole
- Editorials and non-peer reviewed articles
- Articles not available in English
- Articles, that are not fully available

3.2 Pilot study

After performing the pilot study, the following digital libraries were selected, since they returned the best criteria matching articles:

- Science Direct (http://www.sciencedirect.com/)
- ACM Digital Library (http://dl.acm.org/)
- IEEE Xplore Digital Library (http://ieeexplore.ieee.org/Xplore/home.jsp)

Based on the pilot study, the search string selected for all databases was (”Internet of Things” OR IoT) AND security. The search string attempted to capture all articles related to the Internet of Things and security.

3.3 Search execution

For each selected database the following steps were taken:

1. A search was performed using the selected search string. The results were sorted by relevance.
2. From each topic, the full citation, abstract and the full text were retrieved.
3. Duplicate articles found previously were discarded.
4. Each topic matching the inclusion criteria was examined further. If the abstract and the metadata did not contradict the exclusion criteria, the article was fully read. If the article was still conforming with the study selection criteria, it was selected.

4 RESEARCH INFORMATION ABOUT THE SECURITY IN THE INTERNET OF THINGS

In this chapter, the research questions 1 and 2 will be answered. Research questions 3, 4 and 5 are so extensive, that they have been divided into their own chapters. Table 2 contains the overall found search results and selected articles per database. From the selected articles the following data was extracted:

- Author(s), date and year
- Publication type and content
    - Conference paper (CP)
    - Workshop paper (WP)
    - Journal article (A)
- The application domain concerned
- The main concerns about the security of IoT
- The proposed solutions for the problems presented (If applicable)

The extracted raw data is listed in the Appendix 1.

Table 2. The number of search results and selected articles per database

Library	**Number of search results found**	**Number of articles selected**
ACM Digital Library	266	4
ScienceDirect	1377	13
IEEE Xplore	1811	23
Total	**3454**	**38**

4.1 RQ1: When and how was this research published?

Figure 3 shows the number of articles published per year from the selected articles. The articles were searched from the beginning of 2006, but the first selected article was from the year 2010. After 2010, there has been a steady increase in the number of articles. Out of the selected articles 20, more than half, were published in 2015. By the end of July of

2016, there have already been almost as many articles published as there was in the whole of 2014. This shows, that the security is currently a major research topic.

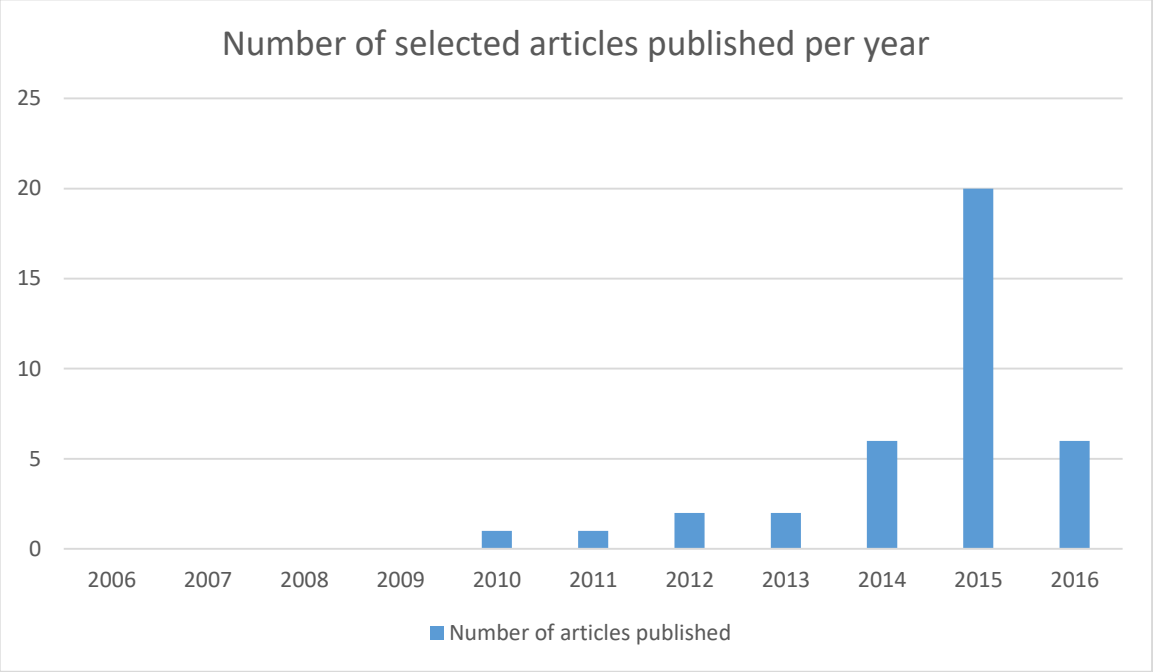

Figure 3. Number of selected articles published per year

Most of the publications are either in conference papers (19) or journal articles (16). Only two of the selected papers were workshop papers. There are no specific publications or conferences where the selected articles were published in. Instead the articles were distributed between different mobile communications, security and traditional networking conferences and journals. The single biggest organization in the selected papers was IEEE with 10 selected articles (26%). This may be in part due to using an IEEE database. There were no single big key conferences or papers.

4.2 RQ2: Which application domains have been researched?

The application domains were selected based on the search results. Each selected article that handled a specific application domain was separated into a category. If the article didn't specifically target a single domain, it was classified under the general category.

Figure 4 shows the number of selected articles per application domain. By far most of the selected articles were not focused on a specific application domain, but instead were general articles about security in the IoT. However, some of the articles were specifically focused on security in some application domains. These issues will be further examined in the following research questions. The general research has been carried out since 2010, while the more specific application domains like smart homes and smart grids are a more recent (since 2015) research subject.

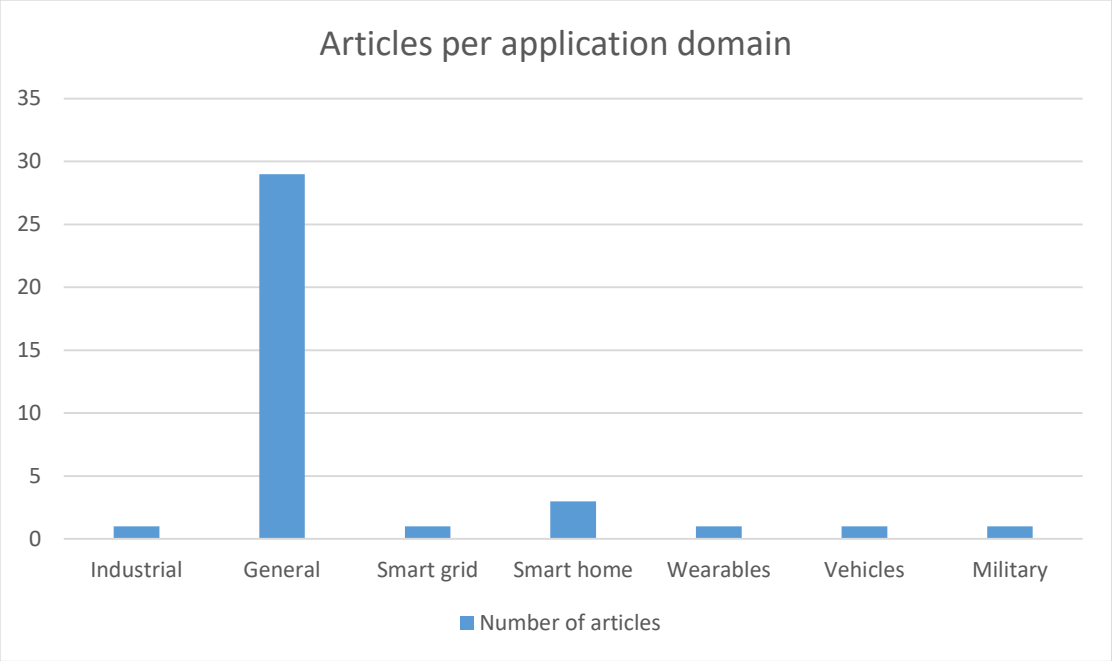

Figure 4. Number of articles per application domain

5 THE SECURITY CONCERNS OF THE INTERNET OF THINGS

In this chapter RQ3 about the security concerns of the IoT is answered. According to many researchers the current security solutions are not suitable to secure the modern IoT environments. Either the approaches are too resource heavy for the IoT or they are simply fundamentally flawed when an IoT environment is considered. In this subchapter, the different concerns raised by the researchers are introduced.

The articles were categorized by hand. After reading the articles, the key points were extracted from them. After the key points were gathered, they were categorized into the broad categories. If a paper had multiple key points, it was added to all of the fitting categories. Table 3 shows a categorization of threats found in the selected papers. These categories are further expanded in the rest of the chapter.

Table 3 The categories of papers

Threat	References
Computational and network constraints	[16] [17]
Privacy concerns	[10] [18]
Identification, authentication, authorization	[10] [19] [20] [21] [22] [23] [24]
Vulnerable devices	[10] [20] [25] [26]
Cross device dependencies	[25]
Lack of enforcement mechanisms	[15] [25]
Many threat sources	[27]
Attacker models	[10] [13] [5] [15] [20] [21] [28] [29] [30]
Legislative issues	[31] [32] [6]

5.1 Security constraints

One of the main challenges of the security in the Internet of things are the constraints set by the environment. Hossain et. al. [16] enumerate them. First they list the hardware

limitations: devices are constrained by computational power, memory and battery. Computationally complex memory intensive operations are therefore not well suited for the IoT.

The software in the IoT devices also has its own limitations. The operating systems embedded into IoT devices have thin network stacks (see Figure 1). This also limits the types of security modules designed for those systems. Another aspect of the embedded operating systems is, that they may not be able to be remotely reprogrammed. This limits the ability to deliver security patches to the systems.

Finally, Hossain et. al. list the network-based constraints. Devices may move from network to network or from sensor to sensor often. This mobility needs to be taken into account, when designing security protocols for the IoT. IoT networks may also be very large. This requires, that the security solutions designed for IoT are also scalable. Furthermore, the IoT devices are very heterogeneous. Security solutions designed for the IoT need to be able to be used by both low-end RFID tags and powerful desktop PCs. These heterogeneous devices also communicate via a wide variety of communication media, both wireless and wired. This increases the difficulty of designing appropriate security for the IoT. To make things even more complex, the communication protocols used in the networks may not always be the standard Internet Protocol (IP). Finally, the dynamic network topology of the IoT presents additional challenges.

Roman et. al. [17] also write about the device constraints of the IoT. They too agree, that the low computational power is a limitation for some current cryptographic mechanisms. They also mention the network security. IoT devices must use the Internet standards for communication, but they lack the resources to implement the currently existing required security measures.

5.2 Privacy concerns

Henze et. al. [18] and Airehrour et. al. [10] write, that the data collected by the IoT devices is often sensitive information, that third parties may be interested in. As an example they

give the telemetry data of a car, which might be of interest to insurance companies, who could use it as a basis to rate hikes or even denying a new contract altogether. According to both articles even more concerns arise, when the data is outsourced to cloud environments. Henze et. al. say, that users don't trust cloud services with the most sensitive of their data, e.g. health information. They also state, that the service providers have their own troubles with sensitive customer data. Not handling this data with the privacy considerations in mind, they may face expensive lawsuits.

Malina et al. [33] also write about privacy problems in the IoT. They too, say that that the IoT data is often of the sensitive sort and needs to be prevented from leaking to third parties. They argue that the problem with the IoT privacy is, that privacy-preserving solutions are designed for powerful computers and use computationally expensive cryptographic primitives. Roman et. al. [19] agree, that one of the main concerns in the security of the IoT are the cryptographic algorithms. They say, that cryptographic algorithms, that provide high throughput in resource constrained devices are needed.

Roman et. al. [19] also state the problem with privacy in the IoT. According to them, users should have tools to retain anonymity and tools to enable transparency. They argue, that IoT itself has to seriously consider the implementation of privacy by design principles and provide user-centric support for security and privacy.

Fink et. al. [34] also identify many privacy concerns. They state, that the involuntary data gathering of location, audio, video and other sensors will likely increase. Location patterns are of interest to advertisers and vendors, but users are hesitant to share their location data intentionally. However, IoT location sensors owned by others can make the sharing implicit. Many devices and applications like Samsung's Smart TV and Apple's Siri listen to the users to provide voice activation mechanisms, and can share this information with the manufacturer.

5.3 Identification, authentication and authorization

Many researchers [20,19,10,21,22,23] argue, that one of the main security concerns in the IoT is device identification and authentication. The massive number of devices in the Internet of Things makes uniquely identifying and authenticating a single device extremely difficult. Without authentication, it is not possible to assure, that the data flow produced by an entity contains what it's supposed to contain. Related to authentication, there's also a problem of authorization. Some sort of access control is required so that everyone is not enabled to access everything in a network.

Nguyen et. al. [24] observe, that very few of the current security protocols offer access control or privacy protection properties. They argue, that especially the access control service is very important in the Internet of Things. They note, that server-based protocols often offer this service with the help of an authorization server.

5.4 Vulnerable devices

According to many researchers [25,20] an important aspect in the IoT security is the device security. Yu et. al. present multiple known vulnerable devices. Some of the devices have their default username and password hardcoded. For example, one camera had its default username and password set as "admin". Other devices had open IPs or ports and protocols that could be accessed. One example is a CCTV setup, which had unprotected RSA key pairs in the firmware for about 30 000 devices. In the list are also a traffic light system, where 219 traffic lights were completely unprotected, allowing malicious users to change the lights at will. The last examples are two smart home products, that ran an open DNS resolver, which could be used to mount Distributed Denial of Service (DDoS) attacks. These devices also contained a vulnerability that allowed connected devices to be accessed from anywhere in the Internet and not just the local network.

Airehrour et. al. [10] write about a case in 2012, where live footage from TRENDNET IP cameras was available to web users without requiring any password. This incident caused the Federal Trade Commission in the United States to announce a need for a secure IoT ecosystem.

Patton et. al. [26] performed and extensive study on the vulnerable devices of the IoT. Their research included 35 737 different devices. The first devices introduced was the iLON SmartServer device. 1258 of these devices were publicly accessible via IPv4 and 45 devices (3,5%) were still using the default username and password. The second device was Niagara SCADA system, used in for example air conditioning and water/wastewater systems, and are used for example in hospitals. 32 248 devices were scanned using http, and out of these devices 150 (0,44%) were using the default username and password. Next, they probed 231 traffic control cameras using a system called PIPS manufactured by 3M. Out of the 231 cameras, 154 (66%) were still accessible via default username and password. Finally, 47 159 printers were scanned, of which 19 583 (41%) were accessible via telnet without requiring authentication.

5.5 Cross device dependencies

Yu et. al. [25] claim that the interconnected nature of the IoT presents additional security risks. They present an example of an attacker disabling an air conditioning unit, which would cause the temperature in a room to rise, which would then trigger another system to open the windows of the room, thus presenting a physical security risk. These interconnected devices are not uncommon. They present a few examples: NEST Protect home system has 188 cross-device policies, Wemo Plugin has 227 and Scout Alarm has 63.

5.6 Enforcement Mechanisms

According to Yu et. al. [25] the enforcement mechanisms of IoT are either broken or lacking. There are no host based defenses, such as antivirus, due to lack of resource on the devices and the heterogeneous nature of the IoT environment. IoT devices also lack the automated software updates of traditional networked devices. The current vulnerability patching happens via firmware updates and that is done per manufacturer and per device. Third, the current network security mechanisms largely rely on strong static perimeter defenses, such as firewalls. When vulnerable IoT devices are embedded deep inside the

network, this approach will no longer be effective. Kumar et. al. [15] are also worried about the lack of security updates in the IoT.

5.7 Sources of threats

Atamli et. al. [27] list sources of threats for the IoT. They are malicious users, bad manufacturers and external adversaries. Malicious users are owners of IoT devices with the potential to perform attacks to learn the manufacturer's secrets and gain access to restricted functionality. The user may then sell the information forward or use it to attack similar systems.

Bad manufacturers produce devices with the ability to exploit technology to gain information about users or other IoT devices. The manufacturers can deliberately introduce security holes, which they can exploit in the future. On the other hand, manufacturer can just unintentionally secure the devices poorly, which may also compromise user security. In addition, in the IoT context manufacturers can develop devices, which will attack other competitor's devices in the same network.

Finally, external adversaries are outside parties, which have no access to the system. The adversary can try to access the system to gain information about the user or the system for malicious purposes. The adversary may also try to disturb the operations of the systems by transmitting his own data to the system.

5.8 Attacker models

In this chapter, many different attacker models against the IoT are introduced.

5.8.1 Denial of Service attacks

Zhang et. al. [35] talk about DDoS attacks against the IoT. DDoS attack is an attack that utilizes multiple computer and attempts to make a service or resource unavailable, usually by generating large numbers of traffic so that the targeted resource is unable to handle everything at once. An IoT environment is even more vulnerable to these kinds of attacks due to its open nature of allowing many different devices in the network. The IoT

workflow is also highly chained. Single point of failure could cascade over the network quickly. According to Zhang. et. al. current DDoS preventive measures rely too heavily on power supply, computing resources and longtime processing, which are not ample in the IoT environment, where low power real-time communications are key.

Roman et. al. [19] and Ashraf et. al. [28] also agree, that Denial of Service (DoS) attacks are a threat to IoT systems. They add, that in addition to the traditional DoS attacks targeting service provider resources, the whole wireless infrastructure can be targeted in the IoT, by for example jamming the used radio channels. Roman et. al. also state, that if an attacker can take control of a part of the infrastructure, they can cause even more mayhem.

Ashraf et. al. [28] also describe a form attack, where after facing continuous DoS and collision attacks, the batteries on the devices become exhausted. Kumar et. al. [15] describe a different sort of an exhaustion attack called sleep deprivation attack. In this attack, the device is prevented from entering into a power-saving mode, by making just enough legitimate requests to keep the device awake.

Ashraf et. al. [28] describe a collision attack as a form of DoS attack. A collision in the network happens when there are multiple signals in the concerned spectrum. Attacker can disrupt network communications by transmitting asynchronously, which may cause checksum mismatches and other problems. An attacker listens to the communications in a channel and guesses the expected time of message transmission. Then the attacker sends a message at the same time, which will result in a collision of the message.

Ashraf et. al. [28] also describe a sinkhole attack. In this attack, the attacker compromises the central node (aka. sink node). This will lead to loss in availability and may even cause a DoS attack, as the sensors try to send data to the central storage.

5.8.2 Physical attacks

Roman et. al. [19] say, that physical damage is one of the security threats in the IoT. Physical damage can be seen as a subset of DoS attacks. In this model, the attacker usually lacks technical abilities and can only hinder the operation of the network by destroying the physical devices. In the IoT this is a very real threat, since the devices (e. g. street lamps) are be easily publicly available. Ashraf et. al. [28] also add, that the "destruction" of the device can be done by simply sending an unauthorized "kill" command to the node.

Related to physical damage, Roman et. al. [19] and Zhao et. al. [5] also state, that node capture is also a threat to IoT security. Instead of destroying the devices, an attacker may attempt to extract the information from the publicly available entities. Attackers may also attempt to capture infrastructure elements, such as data storage and processing entities. Ashraf et. al. [28] call this form of attack "tampering". They also add, that an attacker can also reprogram the device to attack against the network.

Roman et. al. [19] also discuss about controlling entities. If there's an attack path, attackers may try to gain partial or full control over an IoT entity. The severity and the damage caused is dependent on how important to the infrastructure the particular entity is.

5.8.3 Network attacks

According to many researchers [19,28,15,29,16,21], eavesdropping is also a valid security threat. Passive attackers may attempt to target communication channels, like wireless networks, in order to extract data from the network. If an attacker gains access to an infrastructure, they are able to extract information within that infrastructure. Ashraf et al. add that, eavesdropping is often a prerequisite for other attacks. Kumar et. al. [15] also describe a sniffing attack. In this attack malicious sensors or devices are placed next to the normal sensors and devices, in order to gather information from the normal devices.

Airehrour et. al. [10] write about the security threats to the routing protocols of the IoT. During the route discovery or route forwarding phases malicious nodes can do damage to the network. One example of such an attack is a routing table overflow attack. In this

attack a malicious node transmits a large number of false routing information to neighbors in a manner, that will cause the neighbors routing table to overflow. Afterwards, the neighbor's routing table is in such a state, that it cannot transmit to the real routes. Malicious nodes can also advertise false routes and during node maintenance transmit incorrect false route errors, which can trigger costly route maintenance operations. According to Airehrour et. al. there are no security standards for the routing of the IoT. Ashraf et. al. [28] describe a similar Sybil attack as an attack in which a single node creates its own multiple identities and presents them to the network to gain disproportionately large influence. This may affect adversely to the neighboring nodes, since their routing tables will be filled with the single node instead of the original neighbors.

Ashraf et. al. [28] describe Hello flood as a form of an attack. Some routing protocols require nodes to broadcast hello messages in order to announce themselves to neighbors. If a node receives a hello message, it may assume that the broadcaster is within its radio range and use it as a communication path. However, an attacker may use high power broadcasting equipment to convince every node in the network that the attacker is their neighbor. This will lead to devices trying to send their data packages to the far away attacker and thus cause packet loss.

Another routing attack according to Ashraf et. al. [28] is the gray hole attack. In the gray hole attack a node refuses to forward some packets and just drops them. This may result in a delay and bandwidth degradation in the whole network.

5.8.4 Encryption attacks

Andrea et. al. [13] define some encryption attacks, which are targeting the encryption scheme used in an IoT system. Using a side channel attack, an attacker may obtain the encryption key from the devices. In side channel attack, the attacker utilizes techniques like timing or fault and electromagnetic analysis. Another type of encryption attack is the cryptanalysis attack. In this attack, an attacker already possesses either the ciphertext or the plaintext and is trying to find the encryption key from that data. Finally, they list the man-

in-the-middle attack, in which an attacker positions himself between two communication parties and attempts to capture the key exchange between the parties.

5.8.5 Spamming

According to Razzak [30], spamming is defined as an "act of spreading unsolicited, anonymous and unrelated mass content over the Internet". In the context of the Internet of Things, Razzak says, spamming is essentially placing new 2D barcodes on objects or modifying existing ones, to point to unrelated resources in the Internet and flooding the physical space with the barcodes to increase traffic. Public spots like train stations are extremely vulnerable to this kind of spamming, but even semi-private spaces such as universities face the spam problem.

Razzak [30] states, that in addition to mass flooding physical space with the barcodes, spammers can also employ other techniques. For example, the spammer may create a bar code, that first goes to the location the spammer wants the user to go to and then redirect him to the legitimate resource afterwards. Spammers can also create business cards with false barcodes, to trick users to go where the spammer wants them.

5.9 Concerns in specific application domains

In this subchapter, the specific application domains discussed in the papers are introduced. This chapter answers the RQ3.1.

5.9.1 Industry

Sadeghi et. al. [36] write about the security and privacy challenges in the industrial internet of things. In factories, the Internet of Things can be used to connect independently operated production systems with each other and conventional IT business IT systems. This industrial IoT enables more efficient production and better individualization of products. However, this new smart factory faces also new threats.

Integrating new IT components is followed by integration of countermeasures against cyberattacks with some delay. This means that many smart factories are currently vulnerable to many cyberattacks. In the past different worms and viruses have infected many factories and power plants. The most famous cyberattack is probably the Stuxnet worm, which made centrifuges at an Iranian nuclear facility to fail. Stuxnet may indicate a new trend towards a targeted sabotage against factories by powerful adversaries.

Smart factories consist of many different cyberphysical production systems, which interact with humans and each other via various network connections. Each of these systems offer attack surfaces on various different levels. Electronics are subject to physical attacks, software can be compromised by malicious code, communication protocols are vulnerable to protocol attacks, and even humans can be tricked by phishing and social engineering.

The most important requirement in the industrial environment is availability, so that there are no delays in production. This means that the protection against DDoS attacks is of utmost importance. Another important objective is to prevent any damage to humans. This means that the integrity of the IoT systems has to be preserved. The systems have to be protected against sabotage and unintended use of counterfeit components. Malicious attacks can’t be allowed to propagate within the factory. The confidentiality of the data, code and configuration of the factory systems is important.

5.9.2 Smart grid

According to Bekara [37] smart grid is like the classic power grid augmented with massive use of information technology. In smart grid there are two flows: electric flow and information flow. Electric flow is the main flow of the classic power grid: electricity from the power plat to the customer. Information flow on the other hand is a large-scale two-way flow between all the different shareholders and components, such as smart meters, of the smart grid.

Bekara [37] states that adding the ICT dimension to the power grid, adds also new security issues and challenges. These challenges are mainly the same ones that other IoT based solutions face:

- **Impersonation** - An attacker could impersonate another household's energy meter in order to make it pay for the attacker's energy consumption
- **Eavesdropping/Privacy** - Attacker could find out the energy consumption of other households. This information could be used for example to find out when the owners of a household are on vacation.
- **Data tampering** - Attacker could modify the exchanged data, such as dynamic prices
- **Authorization/Access control** - Remote manipulation of devices could enable attacker to cause physical harm to e.g. transformers
- **Availability/DoS attacks –** Unlike traditional power grid, in smart grid vital parts of the grid are open to denial of service attacks

5.9.3 Smart home

According to Arabo [38], the weakest link in any IT security chain is the user. He says that home users generally assume, that everything will work out-of-the-box, with the default security settings in place. At home the security requirements exceed beyond computers. There are mobile phones, game consoles and car navigation systems, all of which could be exploited by an attacker.

Arabo [38] writes, that attacks to home infrastructures will come in two ways: either by sensors/devices connected to the network or by servers in the network. He says, that the sensors and devices connected to the Internet are the weakest link. Arabo lists multiple security threats against home systems. These include lost or stolen devices, open WiFi networks, malware and viruses and theft of services.

Jacobsson et. al. [39] also write about the risks of smart home automation systems (SHAS). They performed a risk analysis on a SHAS and identified 32 risks. In the risk analysis, the

SHAS was divided into five categories: software, hardware, information, communication and human factor. Out of the 32 identified risks, 9 were classified as low and 4 as high, meaning that most of the risks were considered moderate. The risks classified as high were either related to the human factor (sloppy/gullible end users, poor passwords) or software components, especially Application Program Interfaces (API) and mobile software security. The highest ranked risks were the inadequate authentication and access control configuration in the in-house gateway.

5.9.4 Military

Wrona [40] discusses about the Internet of Things in the military context. In military, the IoT can be used for many different things. Smart equipment like vehicles, supplies and weapons systems can all utilize the IoT. However, there have already been identified many several vulnerabilities in cars and there are known examples of the enemy exploiting the weaknesses of military cyberphysical systems. There are also known vulnerabilities in the current smart rifle technology.

IoT can also be used for situational awareness. Adding civilian IoT technology into military IT systems could improve the operational picture available to commanders. Such positive effect however can only be achieved if there's enough guarantee of availability and integrity of the information.

In logistics, the use of RFID can improve the efficiency of operations, for example when operating with third-party logistics systems. The improved efficiency can also be used to improve security to prevent e.g. the joint transportation of dangerous chemicals or critical parts of cryptographic equipment. On the other hand, the improper integration of RFID tracking in the backend could lead to new attack paths. In addition, lack of confidentiality could enable the enemy to perform better targeted attacks on the logistics operations or use the logistics information to infer planned military operations. Lack of integrity could allow the adversary to harm the logistics operations by rerouting convoys etc.

Finally, the IoT could be utilized in medical care. Soldier's health information could be implanted into their uniforms or even in the literal implants they may have. This could improve the speed and accuracy of delivering medical care to soldiers. This technology also possesses risks: many medical devices have been demonstrated to have security vulnerabilities.

5.9.5 Wearable devices

Arias et. al. [41] write about the privacy and security concerns in wearable devices. As a case study, they use the Nike+ Fuelband fitness tracker. The fitness tracker uses a Bluetooth interface to communicate with a smartphone. Firmware updates are however performed using a Nike+ application on a personal computer. However, the tracker did not utilize all of the security capabilities of its micro-processor and they were able to extract the firmware, modify it and upload it back to the device, thus compromising it.

Arias et. al. further write about the consequences of such attacks. The compromised devices could be used to disrupt networks, cause physical harm to their users and compromise their security. This is further emphasized in the context of wearable devices, since these devices often collect very sensitive information about their users. If this information were to be leaked, it could cause serious consequences.

5.9.6 Vehicles

Sun et. al. [42] discuss about the security issues in the Internet of Vehicles (IoV). In vehicles, the Internet can be used to communicate between vehicles, from the vehicle to the road, from vehicle to human and from vehicle to sensor. These communications can be used to improve safety, manage traffic and provide convenience to drivers. There are however multiple security issues in the IoV. Many of them are the same as in the general IoT, but have unique characteristics.

Due to the mobile and dynamic nature of the IoV, vehicles are especially susceptible to the Sybil attack discussed in chapter 5.8.3. Vehicles are also especially vulnerable to GPS attacks. Many vehicular services, such as navigation, rely on GPS information. Spoofing this information may cause serious damage. Masquerading and Wormhole attacks also

provide a threat for the IoV authentication. IoV is also vulnerable to the availability attacks discussed in chapter 5.8.1 and routing attacks discussed in chapter 5.8.3

5.10 Legislative issues

In 2010 Weber [31] argued that new regulatory frameworks will become necessary in order to protect the privacy of the consumers. In 2010 much of the IoT industry was largely self-regulated. Weber argued, that this kind of regulation may not be enough to ensure effective security or privacy. Weber stated that an international regulation would be necessary due to the global nature of the IoT.

However, in his later paper [32] Weber says, that an international regulatory framework is still missing. According to Weber, most laws are only concerned with basic data protection issues, and do not directly address the complex requirements of the IoT. The customer data collection will only become more prevalent and legal issues need to be tackle, so that customers may have control over their own data.

Suo et. al. [6] also note the need of security law and regulations to note the IoT. They state, that the IoT is related to national security, business secrets and personal privacy and thus needs the legislative point of view to promote the development of the IoT. The lack of policy and regulation is urgently needed.

5.11 Summary

In this chapter, the perceived threats against the Internet of things were presented. Table 4 The security concerns of the Internet of Things presents a summary of the findings. In this table the threats are also tied to the different elements of the IoT, which were introduced in chapter 2.2.2 and Figure 2.

Researchers have identified at least some sort of security concerns against almost all of the elements of the IoT. Communication, computation and sensing have the most threats identified against them. No threats are perceived against the semantic element. This may be in part due to the semantic element being more of a data aggregator than producer or

transporter. The attacks against this part of IoT are easier to perform by attacking some other element, so the semantics will produce the wanted behavior based on wrong data or lack of it.

Table 4 The security concerns of the Internet of Things

Threat	Element of the IoT concerned (Figure 2)	References
Computational and network constraints	Communication, Computation	[16] [17]
Privacy concerns	Sensing, Communication, Computation, Services	[10] [18]
Identification, authentication, authorization	Identification, Communication, Services	[10] [19] [20] [21] [22] [23] [24]
Vulnerable devices	Sensing, Communication, Computation	[10] [20] [25] [26]
Cross device dependencies	Sensing, Communication	[25]
Lack of enforcement mechanisms	Computation	[15] [25]
Many threat sources	Sensing, Communication, Services	[27]
Denial of Service attacks	Communication, Computation	[19] [35] [28]
Physical attacks	-	[5] [19] [28]
Network attacks	Communication	[10] [15] [16] [19] [20] [21] [28] [29]
Encryption attacks	Computation	[13]
Spamming	Sensing, Services	[30]
Legislative issues	-	[31] [32] [6]

6 THE SECURITY SOLUTIONS OF THE INTERNET OF THINGS

In this chapter, RQ4 about the security solutions for the IoT is answered. In addition to problems, many researchers have also suggested solutions for the IoT security problems. In this subchapter, the solutions presented in the selected articles are further examined.

As with the previous chapter, these categories were selected by hand. The articles were read and key solution in those articles were extracted. These solutions were then categorized in broad categories and the articles were put into those categories. In Table 5, the categories for the solutions are presented. These are further examined in the rest of this chapter.

Table 5 The solution categories for the IoT

Solution	References
Trust management	[13] [16] [17] [21] [43]
Privacy solutions	[17] [18]
Authentication	[14] [20]
Fault tolerance	[17]
Policy enforcement	[25]
DDoS protection	[35]
Secure communication	[10]
Secure routing	[10]
Spam prevention	[30]
IoT architectures	[44]
Regulatory solutions	[45]

6.1 Trust management

Yan et. al. [43] and Hossain et. al. [16] claim, that trust management plays an important role in the IoT. Having trust management helps people overcome the uncertainty and risks attached to the IoT. Trust as a concept covers both security and privacy aspects of the

systems. The trust management should cover all of the layers of the IoT. To provide trustworthy IoT, they propose that a holistic trust management should achieve the following goals:

- **Trust relationship and decision:** Trust management should provide an effective way of evaluating trust relationships of IoT entities and assist them communicate and collaborate with each other.
- **Data perception trust:** Data sensing and collection should be reliable in the IoT.
- **Privacy perception:** User privacy should be preserved according to the policy and expectation of IoT users.
- **Data fusion and mining trust:** Data should be processed and analyzed in a trustworthy way.
- **Data transmission and communication trust:** Data should be transmitted and communicated securely.
- **Quality of IoT services:** The quality of services should be ensured.
- **System security and robustness:** System attacks should be countered to gain user confidence
- **Generality:** The trust management should be generic, so that it can be widely applied.
- **Human-computer trust interaction:** The device interaction should be trustworthy and usable, so that they can be easily accepted by the users
- **Identity trust:** The identifiers of the IoT entities are well managed, scalable and efficient.

Roman et. al. [17] also agree, that trust is essential for the IoT. They state, that trust is more than the mechanisms that reduce uncertainty. Trust is also about how the users feel when interacting in the IoT. Feelings of helplessness and being controlled can greatly reduce the trust in the IoT. Users must be able to control their own services and have tools to describe their interactions with the systems. They also state, that good governance can increase the trust in the IoT.

Andrea et. al. [13] and Abomhara et. al. [21] also identify some trust relationships. There needs to be trust between each of the layers of the IoT. Communication and transition between the layers need to be secure and private. For each layer of the IoT, there also needs to be trust for security and privacy, meaning that each IoT layer must be preserved under any circumstances. Finally, there needs to be trust between the user and the IoT system.

Abomhara et. al. [21] also discuss other aspects of trust management in the IoT. They state, that the main objectives of trust research in the IoT are the conception of new models for decentralized trust, implementation of trust mechanisms for cloud computing and development of applications based on node trust. They state that trust evaluation should be autonomous and automated.

6.2 Privacy solutions

Roman et. al. [17] offer some solutions for the privacy issues. One of the principles is privacy by design. Privacy by design means, that users would have the tools to manage their own data. For example, user in New York's Central Park could offer the information, that he's in New York, but not that he's in a specific park. Another principle is transparency. Transparency in the context of IoT means that users should know which entities are managing their data and how and when they are using it. Third solution they present is data management. This means deciding who is managing the secrets. Cryptography may protect the data to a certain extent, but such mechanisms don't work in every environment. There has to be various data management policies and a policy-enforcement mechanism.

Henze et. al. [18] present a solution for handling IoT data in cloud environments called User-driven Privacy Enforcement for Cloud-based Services in the IoT (UPECSI). With UPECSI users are able to control their sensitive data, before it is transferred to the cloud. It also allows cloud service developers integrate privacy functionality to the development process of a cloud service. Finally, it provides users a user interface, with which they can configure their personal privacy settings.

6.3 Authentication

Zhang et. al. [20] present multiple authentication models for the IoT. First they suggest an authentication-by-gateway model. In this model, all external devices would have to authenticate via a gateway, before the local devices could communicate with those devices. After authentication, the external device would be directed to the local device until the session terminates. Each time the devices communicate with the external network, the authentication would have to be redone. The downside for this kind of authentication model is that it exposes a single point of failure, which could expose all of the peers to threats.

The second model they introduce is authentication by security token [20]. In this model, the gateway issues a security token with the communicating parties. While the security token is valid, all of the communication between the parties is done using the security token for authentication. This model reduces the load from the gateway introduced in the first model, but still leaves the single point of failure problem present.

Third model is authentication by trust chain [20]. In the trust chain, peer A trusts peer B. When peer A receives data from peer C, it only trusts that the data is from peer C if peer B also confirms that the data is from peer C. The gateway is the root of the trust graph. This reduces even more load from the gateway, since after the initial setup there are no further authentication workload on the gateway. However, there is still a single point of failure, since compromising the gateway may break the trust chain.

Final model introduced is authentication by global trust tree [20]. In this model, all of the peers are registered in a global trust tree, which means that all of the peers may be authenticated globally. However, there are currently no known global trust trees available in the Internet. This would remove the single point of failure of the compromised gateway, since the authentication is managed elsewhere.

Mahmoud et. al. [14] also write about authentication schemes. They present a one-time one cipher method based on request-reply mechanism. The cipher is implemented by using a pre-shared matrix between the communicating parties. The parties generate a random coordinate, which corresponds to a key in the matrix. The coordinate is transmitted between the parties instead of the key itself and this key is then used for creating the ciphertext.

6.4 Fault tolerance

Roman et. al. [17] state some requirements for IoT systems to be fault tolerant. Achieving fault tolerance in the IoT, requires three things. First, all devices must be secure by default. In addition to secure protocols and mechanisms, the software inside the devices must also be secure. The second requirement is to give all IoT objects the ability to know the state of the network and its services. The system would require an accountability system, that monitors the state of the network. Finally, all objects should be able to defend themselves against network failures and attacks. Protocols should include mechanisms that respond to abnormal situations and let the object degrade its service.

Once an attack affects the services, the elements should be able to act quickly and recover from any damage. Elements could use feedback from other mechanisms and entities to map the locations of unsafe zones and trusted zones. This information could be used as a basis for implementing various recovery services and used to notify human operators of any damages.

6.5 Policy enforcement

Yu et. al. [25] present a software based approach to IoT security. Their solution is a security architecture consisting of micro security functions called µmboxes. A high level vision of their solution called IoTSec can be seen in Figure 5. The architecture has a centralized IoTSec controller, that monitors the environment and generates a global view for cross-device policy enforcement. Administrator can configure and instantiate new µmboxes and their routing mechanisms from this view.

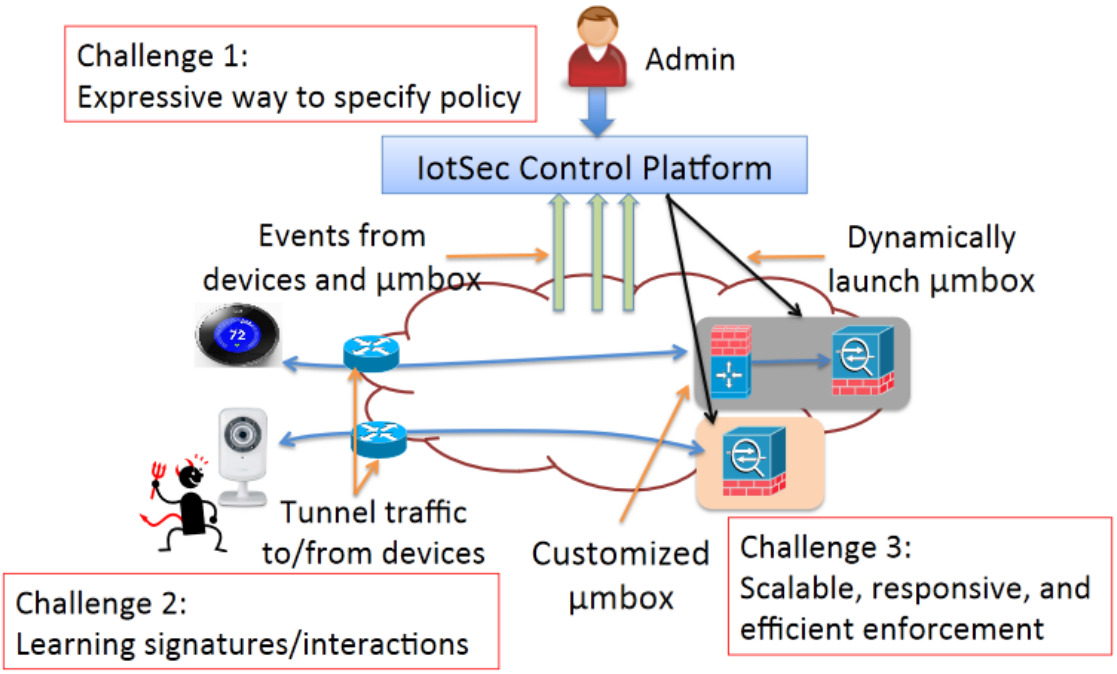

Figure 5. Yu et. al. IoT security platform [25]

6.6 DDoS Protection

According to Zhang et. al. [35] a Learning Automata (LA) has been presented as a solution to DDoS attacks in IoT networks. The LA would intelligently determine the packet sampling rate from the environment. In detection phase the DDoS prevention component in each device would monitor the requests the device receives and once a preset maximum capacity is exceeded, it would issue out a DDoS alert to neighboring nodes. Once the alert is issued, the devices would sample the IP addresses and try to detect the attacker. Once the attacker is identified, other nodes would be notified of this attacker and they would drop any packets arriving from the attacker IP. Based on this approach, Zhang et. al. present their own algorithm for detecting and preventing a DDoS attack in an IoT network. Another approach is to back up the sink node (a node, that receives the data collected by sensors). This new node would be a redundant channel to hold a portion of the responsibilities of the sink node. This approach is considered a cost effective one [35].

6.7 Secure communication

Kumar et. al. [15] state, that the IoT protocol stack will try to match that of the classical Internet hosts, to create an Extended internet. According to them, this enables the IoT to utilize many of the existing security solutions. At network layer, IoT utilizes the Internet Protocol Security (IPSec) to secure data exchange between devices. At the transport level, the communication between nodes can be secured using Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS). The issue with these technologies is that they are dependent on intermediate nodes to assure complete end-to-end security.

Nguyen et. al. [24] also examine secure communication protocols in the context of the Internet of Things. They examine two different categories of security solutions: solutions based on asymmetric keys and solutions that are based on symmetric pre-distributed keys. Both approaches have their advantages and disadvantages.

Asymmetric key schemes can further be divided into two sub-categories: techniques where key transport is based on public key encryption and techniques where the key agreement is based on asymmetric techniques. The first category is similar to the traditional key transport mechanism, while in the second category a shared secret is derived between parties based on asymmetric primitives. The downside of asymmetric keys in the context of Internet of Things is the high computational cost and energy consumption required. However, according to Nguyen et. al. improvements in the cryptographic primitives continue to reduce the cost of cryptographic operations. The definite upside of asymmetric schemes is that they are more resilient to node capture attacks, have lower memory requirements, few message exchanges and high scalability for large networks.

Symmetric schemes with pre-distributed keys can also be divided into two sub-categories: probabilistic key distribution and deterministic key distribution. In the first category mechanisms distribute security credentials chosen randomly from a key pool to nodes. During the initial communication, two nodes may discover a common key with a certain probability. In the deterministic approach, the keys from the key pool are distributed

uniformly so that each two nodes share a common key. The upside of symmetric schemes is that they have low computational requirements. The downside is their high communication complexity, high memory usage, lower scalability and vulnerability against node capture attacks.

6.8 Secure routing

Airehrour et. al. [10] write about secure routing protocols to prevent routing attacks. First they introduce a secure multi-hop routing protocol (SMRP). The protocol requires nodes to authenticate before joining the network. Due to the protocol including a summary of devices allowed into the network in a parameter, it does not work well on a large scale.

Second protocol introduced is a trust-aware secure routing framework in wireless sensor networks (TSFR). TSFR is based on trust derivation, where behavior of nodes is observed directly and indirectly. Based on the observations, nodes are assigned a trust value between 0 (no trust) and 1 (fully trusted). However, TSFR uses a significant amount of memory and malicious nodes are identified based on previous trusts. A rogue node could join the network and behave well for a while and start the malicious behavior afterwards.

Third two-way acknowledgement-based trust (2-ACKT) is introduced. This protocol assumes, that during the routing phase there were no attackers or malicious nodes in the network. The protocol is uses a dual-acknowledgement system to develop trust between two nodes. In the system there’s also a third-party node, that creates a two-hop acknowledgement in the network. The protocol assumes, that malicious nodes will drop the data packets, but not the acknowledgement packets, and thus can’t isolate grey hole attacks.

The fourth protocol is called group-based trust management scheme (GTMS). This protocol also calculates the trust between nodes via observation of node behavior (the number of successful and unsuccessful transactions between nodes). For intra-group communication, Cluster Heads are used with a distributed trust management scheme to gather recommendation from all of the group members and about other Cluster Heads

directly from the sink. To reduce memory consumption, the trust levels are assigned as integers between 0 and a 100. However, Cluster Heads have a high energy requirement, which could quickly drain the sensor batteries.

Finally, a collaborative lightweight trust-based routing protocol (CLT) is introduced. As the name implies, the protocol is based on a collaborative trust effort among nodes, while trying to minimize memory overhead and battery consumption in nodes. The protocol uses a trust counselor, which monitors, warns and improves any node, whose trust level is diminishing. The protocol can't function with autonomous nodes and assumes that all nodes have a unique identity.

6.9 Spam prevention

Razzak [30] suggest that a solution to prevent IoT spam, is to use digital signatures to sign the content in 2D barcodes. The barcode would contain, the original content, digitally signed content and the public key of the barcode creator. The certificates verifying the identity of the creator would be placed in the URL the barcode points to. An application would then check the integrity of the QR code and verify the certificate chain.

6.10 Solutions for specific application domains

In this chapter, the suggested solutions for different application domains are presented. This chapter answers the RQ4.1.

6.10.1 Industry

Adapting current security concepts to smart factories is not easy. Traditional IT security protection primarily protect integrity and confidentiality. In case of cyberattacks, the IT systems are temporarily disabled and restored after the attack is over. In the smart factory scenario this is not possible, since availability is the most important factor. The real-time requirement and lower computational power present also their own challenges. This is why a holistic cybersecurity approach for the industrial IoT is required [36].

Sadeghi et. al. [36] suggest a hardware-enforced isolation for security-critical code and data as an architecture for preserving integrity in a smart factory. In addition, attestation is to be used. Attestation enables the detection of unintended and malicious software modifications. However, attestation is hard to achieve on embedded and real-time platforms. This is why at least some form of hardware support is required.

6.10.2 Smart grid

According to Bekara [37] the solution to the smart grid security problems is implementing security services for the smart grid. He suggests the same solution for the smart grid that are required for the IoT in common: authentication services, data integrity services, confidentiality services, privacy services and authorization/access control services.

6.10.3 Smart home

Han et. al. [46] list security requirements for a smart home system. These are very much the same as for the general IoT. They classify the requirements in three categories: confidentiality, integrity and availability.

For confidentiality they suggest, that all of the private user data must be encrypted during all intra-device communication to prevent outside exposure and all of the encryption keys must be managed securely. To prevent outside replication and modification, all of the identification information must be managed securely. The devices passwords should be required to be complex and required to be changed periodically. Finally, the Home Gateway must use a secure password.

Integrity is preserved by authorizing all of the devices and users before they are connected to the to the network. All of the data and encryption keys must remain untampered and authentic. Data integrity must be provided for all data transmissions to either outside of the system or inside the system. To provide a reliable communication environment, all of the devices have to be mutually authenticated.

For availability, external attack detection capabilities must be provided. Devices must have a software update functionality and security policy settings. To deal with physical status (adding a device, stolen device etc.) a device management system must be provided. Periodical device status monitoring should be provided and any abnormal operations should be reported.

6.10.4 Military

Wrona [40] discusses the IoT as a security enabler for military applications. The information received from the IoT could be used to provide additional security-relevant information to enable context-aware security mechanisms. For example, behavioral biometrics could be used as an input to authentication mechanisms or IoT data could be used to dynamically adapt the security measures based on threat level and operational picture.

Wrona also writes about the concept of Object Level Protection (OLP). OLP was developed to support NATO projects. OLP is "a system-wide standard approach to data protection". It has two fundamental ideas:

1. Protection is applied to individual data objects, instead of collection of data objects and systems
2. Metadata is bound to data objects and used by protection enforcement mechanisms to determine protection requirements for a data object.

6.10.5 Wearable devices

Arias et. al. [41] present solutions to the security problems of wearable devices. In addition to the generic security measures of the IoT devices, wearables must take extra precautions. Arias et. al. say, that the wearable devices must secure all of the update channels. The external reprogrammability of the microcontroller and all of the debug interfaces must be disabled. The microcontrollers also have to be programmed before placing into the circuit board to avoid unnecessary interfaces.

6.10.6 Vehicles

Sun et. al. [42] present the security requirements for the IoV. A high availability is required in the IoV due to its safety-critical nature. The high mobility of IoV entities needs to be considered when designing security for the IoT. Key distribution and the identity of the Certificate Authority need to be determined beforehand. There has to be high error tolerance due to the limited bandwidth and unstable connections. Security and privacy concerns need to be balanced. Many drivers are unwilling to give up their privacy even if it means improved security.

Sun et. al. [42] also discuss the countermeasures for attacks against IoV. They mention intrusion detection systems as one possible solution. Intrusion detection systems collect and analyze information from the network systems for any sings of attack. Intrusion detection systems also utilize honeypots. Honeypots are system resources that are intentionally unprotected to entice attackers to break in to. Based on these attacks, the IDS can build up its own security model. Secure routing protocols discussed in 6.8 are also mentioned. Finally, a good key management system is required.

6.11 IoT architectures

Vasilomanolakis et. al. [44] present multiple architectures for the Internet of Things. The purpose of an IoT architecture is to bridge the gap between the actual devices and virtual entities, which produce services etc. The four presented architectures are Internet of Things Architecture (IoT-A), Building the environment for the Things as a Service (BeTaaS), Open source cloud solution for the Internet of Things (OpenIoT) and Internet of Things at Work (IoT@Work).

IoT-A uses concepts of views and perspectives to guide the generation of architecture instances from business goals. The views and perspectives include information view for static structures and dynamic information flows, performance and scalability perspective and trust and security perspective. In addition, IoT-A contains several architecture independent models, like trust, security and privacy model. For security, IoT-A contains many logical security components: Key Exchange and Management, Identity Management,

Authentication, Authorization, Pseudonymization and Trust & Reputation. In addition, the IoT-A contains a fault handling model for predicting potential failures, detecting existing failures and repairing the system.

BeTaaS is an architecture for running IoT and M2M applications over a local cloud of gateways, which integrate various heterogeneous systems. The architecture has four layers: physical layer, adaptation layer, Things as a Service (TaaS) layer and the service layer. The architecture is addressing the security requirements by providing individual mechanisms for each layer, except the physical one. The security components include key management, authentication and authorization, trust and reputation and failure prevention and recovery components. Even though BeTaaS states privacy as one of key aspects of security, there is no evidence how this requirement is fulfilled.

OpenIoT concentrates on providing cloud-based middleware infrastructure to provide on-request access to IoT and its services. The OpenIoT specification describes two security modules: a security & privacy module and a trust module. The security & privacy module addresses secure messaging, authentication and authorization. OpenIoT relies on Hypertext Transfer Protocol (HTTP) with the TLS protocol to provide secure messaging. Resource constrained devices use IPSec tunnels established by the gateways. OpenIoT does not provide failure avoidance, but focuses on mitigation.

IoT@Work is an architecture designed for the industrial automation domain. The architecture introduces the concept of network slices, which are a combination of virtualization, resource management and security. The network slice is an abstract layer between the physical devices and the applications. IoT@Work provides network security via commonly used technologies. Availability is protected by the virtualization in the network slices, which enables a fast fail-over. Device integrity is addressed by the IoT@Work, but network integrity is not protected. Authentication is provided by the network security mechanisms. Privacy is not addressed, since it’s not an important requirement in an industrial environment.

6.12 Regulatory solutions

According to Weber et. al. [45] write about the regulatory action taken on the Internet of Things. In Europe the concept of the IoT was officially accepted in 2007. In 2009, a 14-point strategic action plan for the IoT was established. In 2012 it was established, that there is significant disagreement between the users and the industry about the data protection issues. In 2013, European company called RAND was entrusted by the European Commission to establish guidelines for the IoT. The company concluded, that the best regulatory approach for the IoT is "soft law". The soft law approach includes standards, supervision and ethical character, but will at the same time ensure enough freedom for the industry.

On the other hand, the situation in America is not as clear. The majority of debates take place within several federal agencies, who are only concerned about specific parts of the IoT. The first serious discussion was initiated in 2013, with the Federal Trade Commission (FTC) asking for comments on the IoT privacy and security. Out of the 27 replies received, more than 60% were against regulation. Later in 2013 a workshop on IoT was held by the FTC. The conclusion of this workshop was that regulation would depend on whether the companies would earn revenue from exclusively selling the IoT devices or if they would profit also from selling the user data.

6.13 Summary

In this chapter, the suggested solutions for the security in the IoT were introduced. Table 6 presents the categories identified in the papers and their relation to the elements of the IoT presented in Figure 2 in chapter 2.2.2. The presented solutions are at this point very high level solutions, such as trust management or IoT architectures. Most of the specific solutions are concerned about the communications security, which is understandable, since it can be seen as the most vulnerable part of the IoT. However, the communication and sensing parts were also identified as vulnerable in chapter 5.11 are not really taken into account on the solution side of things.

Table 6 The security solutions for the Internet of Things

Solution	Element of the IoT concerned (Figure 2)	References
Trust management	All	[13] [16] [17] [21] [43]
Privacy solutions	All	[17] [18]
Authentication	Identification, Communication	[14] [20]
Fault tolerance	All	[17]
Policy enforcement	Communication, Services	[25]
DDoS protection	Communication	[35]
Secure communication	Communication	[10]
Secure routing	Communication	[10]
Spam prevention	Sensing, Computation, Services	[30]
IoT architectures	All	[44]
Regulatory solutions	-	[45]

7 RESEARCH GAPS

Sadeghi et. al. [36] say, that currently there are at least two topics that need further research. The next generation of IoT devices will consist of device swarms. The attestation of these systems, called swarm attestation, is still an open topic. Secure device management for IoT devices is another topic requiring further research. Current security solutions don't scale well with the growing number of devices.

According to Malina et. al. [33], there is still a need for a secure privacy preserving solution for the IoT. The current solutions are too computationally heavy for the resource constrained devices, that the IoT mostly consists of. They argue, that IoT applications need a solution, that is not based on expensive bilinear pairing, produces short signatures and is easy to deploy in memory constrained devices.

Roman et. al. [19] state, that there have been very few advanced in the management of access control policies in the distributed Internet of Things. The existing access control policies can't be applied to the distributed environments, due to scalability and consistency issues. Role-based access control policies using certificates also need an infrastructure for validating those certificates in a cross-domain environment. There are however some workarounds for these problems.

Singh et. al. [47] list multiple research areas, which are still relatively unexplored. They mainly focus on the combination of the Internet of Things and cloud environments. They claim that things like in-cloud data sharing, data combination, auditing cloud security, composite service responsibility and the impact of cloud decentralization are still areas that need more research in order to provide a more secure Internet of Things.

One clear gap based on this research is the research on the semantical element of the IoT. Does the whole network consisting of IoT services have any weak points? Can the semantical decisions be influenced from outside of the intended system? How can the integrity of the service network be secured? These are questions that still remain answered at least in the selected articles.

8 DISCUSSION AND CONCLUSIONS

Based on this research, the security in the internet of things still needs a lot of work before it is ready for a widespread public acceptance. There are many security concerns still present for the IoT. Most prevalent of them are privacy concerns, identification, authentication and authorization concerns and various attack vectors on almost every level of the IoT.

The privacy in the IoT is of utmost importance, since the devices used often collect private, personal data such as health information. However, the privacy solutions in the IoT are still a bit lacking. The currently used security measures don't adapt very well to the heterogeneous and resource constrained environment of the IoT. However, a lot of work has been done to either adapt the current protocols for IoT purposes, or even construct completely new ones for the purpose of lightweight encryption and secure network transmission.

In this author's opinion, the most lacking aspect of the IoT security is currently the authentication and authorization. The amount of devices requires secure identification and authentication of them. After authentication, the access control has to be solved, since not everyone can have access to everything. Many researchers present this as one of the key issues to be solved, but based on this research, a universal, efficient and scalable solution for the authentication issues in the IoT are still missing.

Finally, the multiple attack vectors of the IoT are worrying. In addition to the current threats existing the Internet, there are multiple new vectors presented. The open and public nature of many of the IoT systems make them especially vulnerable to malicious attacks. This is further emphasized by the often poor security deployed into the devices themselves. The communication by radio waves is susceptible to many types of attacks ranging from eavesdropping to outright DoS attacks. This puts extra pressure for the systems to be as error-tolerant as possible.

Compared to the previous reviews done on the subject, the same key areas are still the weak point of security in the IoT. Authentication, authorization and encryption are still key issues. Law and regulations still haven't caught up with the rapidly developing technological environment. Vulnerable devices are still one of the key enablers in the attacks against IoT. However, unlike in previous reviews, the solutions are now more concrete and closer to reality. Lots of research has been done to solve the troubling key issues and the solutions presented in this review could make the IoT more secure once adopted.

9 SUMMARY

In this thesis a systematic literature review about the security in the Internet of Things was performed. Out of the 3454 articles, 38 articles were selected for further review according to the chosen search strategy. The thesis attempted to identify the most prevalent security concerns and possible solutions for those concerns. Additionally, some of the current research gaps were identified.

The Internet of Things is a communication paradigm attempting to connect many aspects of our everyday lives to the Internet. The application areas range from smart homes to smart factories and smart vehicles. However, wherever there's networking or software, there's a possibility for malicious users to compromise security. In the case of the IoT, the consequences may be even more severe than in traditional systems, since the systems are often connected to the physical world.

The current state of the security in the Internet of Things is still very much a work in progress. Vast majority of the articles chosen were published in the past three years. This means, that the security research is in full swing, as the IoT is on the verge of its major public breakthrough. However, there are still many different issues preventing the widespread public acceptance of the IoT. These are mainly concerns of privacy. In addition to the privacy issues, there are many other security concerns for the IoT. These are mainly related to authentication, authorization, poor device security and the amount of attack vectors.

REFERENCES

1. Weiser, M. The Computer for the 21st Century. *Scientific American* 1991, Vol. 265, No. 3, 94-104.
2. Gartner. Inc. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. http://www.gartner.com/newsroom/id/3165317 (accessed Aug 8, 2016).
3. Global Standards Initiative. Internet of Things Global Standards Initiative. http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx (accessed Aug 8, 2016).
4. Kumar, S. J., Patel, D. R. A Survey on Internet of Things: Security and Privacy Issues. *International Journal of Computer Applications* 2014, Vol. 90, No. 11, 20-26.
5. Zhao, K., Ge, L. A Survey on the Internet of Things Security. *Computational Intelligence and Security (CIS), 2013 9th International Conference on* , Leshan, 2013; pp 663-667.
6. Suo, H., Wan, J., Zou, C.; Liu, J. Security in the Internet of Things: A Review. *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on* , Hangzhou, 2012; pp 648-651.
7. Atzori, L., Iera, A.; Morabito, G. The Internet of Things: A survey. *Computer Networks* 2010, Vol. 54, No. 15, 2787-2805.
8. Li, S., Xu, L. D.; Zhao, S. The internet of things: a survey. *Information Systems Frontiers* 2015, Vol. 17, No. 2, 243-259.
9. Kitcheman, B., Charters, S. Guidelines for performing systematic literature reviews in software engineering. *EBSE Technical Report EBSE-2007-01*, 2007.
10. Airehrour, D., Gutierrez, J.; Ray, S. K. Secure routing for internet of things: A survey. *Journal of Network and Computer Applications* 2016, *66*, 198-213.
11. Bishop, M. What is computer security? *IEEE Security & Privacy* 2003, Vol. 99, No. 1, 67-69.
12. Al-Fuqaha, Guizani, M., Mohammadi, M., Aledhari, M.; Ayyash, M. Internet of

Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials* 2015, Vol. 17, No. 4, 2347-2376.

13. Andrea, I., Chrystomou, C.; Hadjichristofi, G. Internet of Things: Security vulnerabilities and challenges. *2015 IEEE Symposium on Computers and Communication (ISCC)* , Larnaca, 2015; pp 180-187.
14. Mahmoud, R., Yousuf, T.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* , London, 2015; pp 336-341.
15. Kumar, S. A., Vealey, T.; Srivastava, H. Security in Internet of Things: Challenges, Solutions and Future Directions. *2016 49th Hawaii International Conference on System Sciences (HICSS)* , Koloa, 2016; pp 5772-5781.
16. Hossain, M., Fotouhi, M.; Hasan, R. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. *2015 IEEE World Congress on Services* , New York City, 2015; pp 21-28.
17. Roman, R., Najera, P.; Lopez, J. Securing the Internet of Things. *Computer* 2011, Vol. 44, No. 9, 51-58.
18. Henze, M., Hermerschmidt, L., Kerpen, D., Häußling, R., Rumpe, B.; Wehrle, K. A comprehensive approach to privacy in the cloud-based Internet of Things. *Future Generation Computer Systems* 2016, *56*, 701-718.
19. Roman, R., Zhou, J.; Lopez, J. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks* 2013, Vol. 57, No. 10, 2266-2279.
20. Zhang, Z.-K., Cho, M. C. Y.; Shieh, S. Emerging Security Threats and Countermeasures in IoT. *ASIA CCS '15 Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security* , Singapore, 2015; pp 1-6.
21. Abomhara, M., Køien, G. M. Security and privacy in the Internet of Things: Current status and open issues. *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on* , Aalborg, 2014; pp 1-8.
22. Basu, S. S., Tripathy, S.; Chowdhury, A. R. Design challenges and security issues in the Internet of Things. *Region 10 Symposium (TENSYMP), 2015 IEEE* , Ahmedabad,

2015; pp 90-93.

23. Čisar , P., Čisar , S. M. General vulnerability aspects of Internet of Things. *Computational Intelligence and Informatics (CINTI), 2015 16th IEEE International Symposium on* , Budapest, 2015; pp 19-21.
24. Nguyen, K. T., Laurent, M.; Oualha, N. Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks* 2015, *32*, 17-31.
25. Yu, T., Sekar, V., Seshan, S., Agarwal, Y.; Xu, C. Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things. *HotNets-XIV Proceedings of the 14th ACM Workshop on Hot Topics in Networks* , Philadelphia, 2015; p Article No. 5.
26. Patton, M., Gross, E., Chinn, R.; Forbis, S. Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things. *Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint* , The Hague, 2014; pp 232-235.
27. Atamli, A. W., Martin, A. Threat-Based Security Analysis for the Internet of Things. *Secure Internet of Things (SIoT), 2014 International Workshop on* , Wroclaw, 2014; pp 35-43.
28. Ashraf, Q. M., Habaebi, M. H. Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications* 2015, *49*, 112-127.
29. Benabdessalem, R., Hamdi, M.; Kim, T.-H. A Survey on Security Models, Techniques, and Tools for the Internet of Things. *Advanced Software Engineering and Its Applications (ASEA), 2014 7th International Conference on* , Haikou, 2014; pp 44-48.
30. Razzak, F. Spamming the Internet of Things: A Possibility and its probable Solution. *Procedia Computer Science* 2012, *10*, 658-665.
31. Weber, R. H. Internet of Things – New security and privacy challenges. *Computer Law & Security Review* 2010, Vol. 26, No. 1, 23-30.
32. Weber, R. H. Internet of things: Privacy issues revisited. *Computer Law & Security Review* 2015, Vol. 31, No. 5, 618-627.
33. Malina, L., Hajny, J., Fjdiak, R.; Hosek, J. On perspective of security and privacy-preserving solutions in the internet of things. *Computer Networks* 2016, *102*, 83-95.

34. Fink, G. A., Zarzhitsky, D. V., Carroll, T. E.; Farquhar, E. D. Security and privacy grand challenges for the Internet of Things. *Collaboration Technologies and Systems (CTS), 2015 International Conference on* , Atlanta, 2015; pp 27-34.

35. Zhang, C., Green, R. Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network. *CNS '15 Proceedings of the 18th Symposium on Communications & Networking* , 2015; pp 8-15.

36. Sadeghi, A.-R., Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. *DAC '15 Proceedings of the 52nd Annual Design Automation Conference*, San francisco, 2015; p Article No. 54.

37. Bekara, C. Security Issues and Challenges for the IoT-based Smart Grid. *Procedia Computer Science* 2014, *34*, 532-537.

38. Arabo, A. Cyber Security Challenges within the Connected Home Ecosystem Futures. *Procedia Computer Science* 2015, *61*, 227-232.

39. Jacobsson, A., Boldt, M.; Carlsson, B. A risk analysis of a smart home automation system. *Future Generation Computer Systems* 2016, *56*, 719-733.

40. Wrona, K. Securing the Internet of Things a military perspective. *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on* , Milan, 2015; pp 502-507.

41. Arias, O., Wurm, J., Hoang, K.; Jin, Y. Privacy and Security in Internet of Things and Wearable Devices. *IEEE Transactions on Multi-Scale Computing Systems* 2015, Vol. 1, No. 2, 99-109.

42. Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Xu, J.; Xiong, Y. Security and Privacy in the Internet of Vehicles. *2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)* , Beijing, 2015; pp 116-121.

43. Yan, Z., Zhang, P.; Vasilakos, A. V. A survey on trust management for Internet of Things. *Journal of Network and Computer Applications* 2014, *42*, 120-134.

44. Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A.; Kikiras, P. On the Security and Privacy of Internet of Things Architectures and Systems. *2015 International Workshop on Secure Internet of Things (SIoT)* , Vienna, 2015; pp 49-57.

45. Weber, M., Boban, M. Security challenges of the Internet of Things. *2016 39th*

International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) , Opatija, 2016; pp 638-643.

46. Han, J.-H., Jeon, Y.; Kim, J. Security considerations for secure and trustworthy smart home system in the IoT environment. *Information and Communication Technology Convergence (ICTC), 2015 International Conference on* , Jeju, 2015; pp 1116-1118.
47. Singh, J., Pasquier, T., Bacon, J., Ko, H.; Eyers, D. Twenty Security Considerations for Cloud-Supported Internet of Things. *IEEE Internet of Things Journal* 2015, Vol. 3, No. 3, 269-284.

APPENDIX 1

Table 7. Selected articles from the ACM Digital Library

Author & reference	Year	Pub. type	Domain	Concerns	Solutions
Sadeghi et. al. [36]	2015	CP	industrial	Attacks and attack surfaces of the industrial systems	Security architectures, integrity verification, secure device management
Zhang et. al [35]	2015	CP	general	Distributed denial of service (DDoS) attacks	DDoS detection and prevention algorithm
Yu et. al. [25]	2015	WP	general	vulnerable devices, cross-device dependencies, broken security enforcement	Security policy abstraction, attack detection, dynamic security enforcement
Zhang et. al [20]	2015	CP	general	Naming, identity management, and authentication on application level	Multiple authentication models

(continues)

Appendix 1 (continues)

Table 3. Selected articles from the ScienceDirect

Author & reference	Year	Pub. type	Domain	Concerns	Solutions
Weber, R. H. [32]	2015	A	general / legislative	Privacy in the IoT, amount of data collected, lack of regulation	Industry standards to limit the use and collection of data, regulatory framework to enforce the standards
Henze et. al. [18]	2016	A	general	Privacy of the end users and service providers	Fully configurable privacy framework
Razzak, F. [30]	2012	A	general	Spamming the IoT / tricking the users	Digital signatures
Malina et. al. [33]	2016	A	general	Cryptographic solutions are not lightweight enough for the IoT	N/A
Bekara, C. [37]	2014	A	smart grid	Wide array of issues and challenges preventing the adoption of smart grid	Authentication, data integrity, confidentiality, privacy and authorization services
Nguyen et. al. [24]	2015	A	general	The current security protocols are not applicable to the IoT	Lightweight options, such as public key cryptography, better for the IoT

(continues)

Appendix 1 (continues)

Table 3 (cont.). Selected articles from the ScienceDirect

Author & reference	Year	Pub. type	Domain	Concerns	Solutions
Arabo, A. [38]	2015	A	smart home	The security of smart home devices is lacking and will lead to problems in the future	N/A
Roman, et. al. [19]	2013	A	general	Denial of Service (DoS) attacks, physical damage, eavesdropping, node capture, control of the IoT entities	Protocol and network security, identity management, privacy, trust & governance, fault tolerance
Weber, R. [31]	2010	A	general / legislative	Legislation of the security of IoT is not up to the expected privacy and security standards	International regulation of the IoT
Jacobsson et. al. [39]	2016	A	smart home	32 identified risks of which 4 severe and 19 moderate	Design of smart homes requires
Airehrour et. al. [10]	2016	A	general	Identifies multiple security issues in the routing of IoT	A low power routing protocol for the IoT
Ashraf et. al. [28]	2015	A	general	The vulnerability of IoT requires an autonomic model	Autonomic approaches to security in the context of IoT

(continues)

Appendix 1 (continues)

Table 3 (cont.). Selected articles from the ScienceDirect

Author & reference	Year	Pub. type	Domain	Concerns	Solutions
Yan et. al. [43]	2014	A	general	IoT poses new issues to trust management	A holistic trust management framework for IoT

(continues)

Appendix 1 (continues)

Table 4. Selected articles from the IEEE Xplore

Author & reference	Year	Pub. type	Domain	Concerns	Solutions
Wrona, K. [40]	2015	CP	military	IoT provides a new attack surface in the military IT system	Object Level Protection, cryptographic access control
Arias et. al. [41]	2015	A	wearables	Reliance on vendor designs, closed software, weak or bad cryptography, supply chain threats	Trusted certificates, better cryptography, more secure firmware and software update process
Kumar et. al. [15]	2016	CP	general	Lots of security issues in all of the IoT layers	Lots of technologies already developed to solve these issues
Patton et. al. [26]	2014	CP	general	High number of vulnerable devices out in the wild could cause severe damage	N/A
Suo et. al. [6]	2012	CP	general	IoT contains both the security threats of the Internet and its own internal communication	More research to solve the outlying problems

Appendix 1 (continues)

Table 4 (cont.). Selected articles from the IEEE Xplore

Author & reference	Year	Pub. type	Domain	Concerns	Solutions
Benabdessalem et. al. [29]	2014	CP	general	Wireless communication raises lots of security threats	Lots of technologies already developed to solve these issues
Hossain et. al. [16]	2015	CP	general	Lots of attack surfaces	N/A
Andrea et. al. [13]	2015	CP	general	All of the IoT layers face attacks	All of the layers need to be protected
Weber et. al. [45]	2016	CP	general	Security, privacy, varied devices, network capacities, large quantities of data, regulatory frameworks	N/A

(continues)

Appendix 1 (continues)

Table 4 (cont.). Selected articles from the IEEE Xplore

Author & reference	Year	Pub. type	Domain	Concerns	Solutions
Roman et. al. [17]	2011	A	general	Cryptography, protocols, data and identity management, privacy, self-management, and trusted architectures, regulatory frameworks	N/A
Vasilomanolakis et. al. [44]	2015	CP	general	Proposed IoT architectures are still lacking many security features	Need to address gaps in identity management, privacy and trust
Fink et. al. [34]	2015	CP	general	Existing Internet protocol vulnerabilities, lack of analysis tools and social challenges	IoT ecosystems should provide incentives to users to secure their data, governments should establish global security standards

(continues)

Appendix 1 (continues)

Table 4 (cont.). Selected articles from the IEEE Xplore

Author & reference	Year	Pub. type	Domain	Concerns	Solutions
Mahmoud et. al. [14]	2015	CP	general	IoT layer is susceptible to attacks at each layer, current research mainly focused on auth. & access control	Incorporate new networking protocols, focus on end-to-end security, trust management, global policies and standards, identification
Atamli et. al. [27]	2014	WP	general	IoT has many threats and many attack vectors	Focus on security architecture, middleware and frameworks
Basu et. al. [22]	2015	CP	general	Heterogenity, connectivity, mobility, addressing, resource constraints, discovery	A security framework addressing the issues
Han et. al. [46]	2015	CP	smart home	Confidentiality, integrity and availability of a smart home system	Set of security functions for the smart home

(continues)

APPENDIX 1 (continues)

Table 4 (cont.). Selected articles from the IEEE Xplore

Author & reference	Year	Pub. type	Domain	Concerns	Solutions
Čisar et. al. [23]	2015	CP	general	Insecure interfaces, communication, authentication, privacy, software, poor physical security, poor configurability	Security by design, policies, access control, monitoring, data minimization
Zhao et. al. [5]	2013	CP	general	Each layer of IoT contains multiple security threats	Each layer also has multiple possible answers to these problems
Singh et. al. [47]	2015	A	general	Data transport & mgmt.., identity mgmt., scale, malicious “things”, trust, regulation, decentralization	N/A
Abomhara et. al [21]	2014	CP	general	Privacy, authentication, trust mgmt, Authorization, access control, end-to-end security	Security and privacy must be taken seriously, identify & classify IoT, design architecture standards, develop security frameworks

(continues)

APPENDIX 1 (continues)

Table 4 (cont.). Selected articles from the IEEE Xplore

Author & reference	Year	Pub. type	Domain	Concerns	Solutions
Sun et. al. [42]	2015	CP	vehicles	Authentication, availability, secrecy, routing, data authenticity	A threat model, intrusion detection system, honeypot, secure routing, key management