



Norwegian University of
Science and Technology

Security evaluation of communication interfaces on smart meters

Henrik Willett

Master of Science in Communication Technology

Submission date: June 2018

Supervisor: Karin Bernsmed, IIK

Norwegian University of Science and Technology

Department of Information Security and Communication Technology

Title: Security evaluation of communication interfaces on smart meters

Student: Henrik Willett

Problem description: Conduct a security evaluation of communication interfaces on smart meters. The goal is to find out if the technology used for communication on smart meters provide adequate security to protect assets in the grid infrastructure.

Responsible professor: Karin Bernsmed, NTNU

Supervisor: Martin Gilje Jaatun, SINTEF

Abstract

By 2019, almost all households in Norway will have a smart meter installed. The digitization of the electrical grid may create new vulnerabilities to the critical infrastructure. In this thesis, we evaluated the security in communication interfaces on smart meters. The reason for our research is that we wanted to find out if the technology used for communication on smart meters provide adequate security to protect assets in the grid infrastructure. To answer this question, we conducted a literature review of technology used in Advanced Metering Infrastructure (AMI) solutions and smart meters and an analysis of a smart meter used in Norway. The findings were used to create a threat model and risk analysis to scope down potential vulnerabilities to test. Our findings suggest that confidentiality of communication between the smart meter and Head End System (HES) is maintained. It is protected using application layer encryption based on AES-128 CBC mode. The integrity of communication may be vulnerable because some of the messages are integrity protected using CRC16-CCITT. Data from the Home Area Network (HAN) interface is currently not encrypted which may pose a threat to the confidentiality of a user's consumption data. This thesis is a contribution to increased security awareness surrounding the implementation of smart meters in Norway.

Sammendrag

Alle strømkunder i Norge får installert nye smarte strømmålere innen 1. januar 2019. Digitaliseringen av strømnettet kan introdusere nye sårbarheter til den kritiske infrastrukturen. I denne oppgaven ønsker vi å evaluere sikkerheten i kommunikasjonsgrensesnittene til smarte strømmålere. Hensikten med arbeidet er å finne ut om det er implementert tilstrekkelig sikkerhetsløsninger i kommunikasjonsgrensesnittene slik at ressurser i strømnettet blir ivaretatt. Arbeidet består av en litteraturnomgang av teknologi brukt i Avanserte Måle- og Styringssystemer (AMS) og smarte strømmålere. Vi har videre utført en analyse av en strømmåler solgt til det norske markedet. Litteraturnomgangen og analysen ble brukt til å lage en trusselmodell og risikoanalyse for å identifisere mulige sårbarheter å teste. Resultatene fra arbeidet tyder på at konfidensialitet blir opprettholdt for kommunikasjon mellom den smarte strømmåleren og nettselskapet. All kommunikasjon blir kryptert på applikasjonslaget med en algoritme basert på AES-128 CBC. Integriteten til kommunikasjonen kan være sårbar fordi noen meldinger blir integritetsbeskyttet med CRC16-CCITT. Data fra HAN-grensesnittet er foreløpig ikke kryptert. Dette kan utgjøre en trussel mot konfidensialiteten til forbruksdata fra kunder. Formålet med denne oppgaven er å øke bevisstheten rundt sikkerhet når det gjelder installasjonen av smarte strømmålere i Norge.

Preface

I would like to thank my Responsible professor Karin Bernsmed and supervisor Martin Gilje Jaatun for their help for my thesis. I would also like to thank Anders Been Wilhelmsen for his contribution to the practical testing in this thesis.

At last, I would like to thank my parents for their continued support throughout life.

Contents

List of Figures	xi
List of Tables	xv
1 Introduction	1
1.1 Motivation	1
1.2 Statement of the problem	3
1.3 Methodology	3
1.4 Limitations	5
1.5 Thesis structure	5
2 Literature review	7
2.1 Electrical grid	7
2.1.1 Grid infrastructure	8
2.1.2 Organization of the electrical grid	11
2.1.3 Electricity market	11
2.2 Smart grid	12
2.3 Advanced Metering Infrastructure	14
2.3.1 Purpose of AMI	14
2.3.2 Architecture and components	15
2.3.3 Communication	19
2.4 Security in AMI	20
2.4.1 Introduction to information security	21
2.4.2 Importance of security	24
2.4.3 Threat model of AMI	25
2.4.4 Motivation for attacks	31
2.5 GPRS security for smart meters	38
2.5.1 GPRS overview	38
2.5.2 Security in GPRS	39
2.5.3 Assessment of GPRS Security	42
2.6 UMTS security for smart meters	47
2.6.1 UMTS infrastructure	47

2.6.2	MITM attack on UMTS	48
2.6.3	Feasibility of the attack	48
2.6.4	Countermeasures	50
3	Analysis	51
3.1	Security solution for communication interfaces	51
3.1.1	Communication chain	51
3.2	Key management	55
3.2.1	Aidon Factory System	55
3.2.2	Head-End System	55
3.3	Physical device security	55
3.3.1	Sealing and tampering	56
3.4	Security analysis of specifications	56
3.4.1	Local communication security	56
3.4.2	End-to-end and RF NAN security	57
3.5	Authentication to HES	59
3.5.1	RADIUS protocol	59
3.6	Physical inspection of smart meter	63
3.6.1	Components on circuit board	69
3.7	Risk analysis	70
3.7.1	Business assets	71
3.7.2	Risk matrix	71
3.7.3	Business risks	73
3.7.4	Technical risks	74
3.7.5	Testing plan	75
4	Testing	79
4.1	Test C.1, C.2, and C.8	79
4.1.1	Equipment	79
4.1.2	Setup	80
4.1.3	Method	83
4.1.4	Results	84
4.2	Test C.3, C.4, and C.8	91
4.2.1	Equipment	91
4.2.2	Setup	91
4.2.3	Method	93
4.2.4	Results	95
4.3	Test C.5	95
4.3.1	Equipment	95
4.3.2	Setup	98
4.3.3	Method	100
4.3.4	Results	106

5	Discussion	107
5.1	HAN interface	107
5.1.1	Sniffing data	107
5.1.2	Uploading files	107
5.1.3	Shell access	108
5.1.4	Symmetric key management	108
5.1.5	Activation of HAN port	110
5.2	RS232 interface	110
5.3	MITM attack	110
5.3.1	RADIUS issues	110
5.3.2	Proprietary security solution	112
5.3.3	Mobile communication	112
5.4	Consequences of attacks	113
5.4.1	Exposure of data from the HAN interface	113
5.4.2	Exposure of data from a MITM attack	115
5.4.3	Denial of Service from a MITM attack	115
5.4.4	Motivation for exploiting technical risks	115
5.5	Future security	116
6	Conclusion	117
A	Appendix	119
A.1	shell_script.txt	119
	References	121

List of Figures

2.1	The life cycle of electricity can be separated into three stages: production, transmission, and consumption.	8
2.2	The hierarchical topology of the electric grid is reverse proportional, and can be compared to a tree graph.	9
2.3	The supply of electricity can be separated into five stages.	9
2.4	Overview of the energy market.	11
2.5	The smart grid will interconnect more elements in the power grid, moving away from the traditional hierarchical topology.	13
2.6	Overview of the AMI.	16
2.7	The system module has several connection interfaces depending on the model.	18
2.8	Overview of the internal architecture of Aidon's 6000 series meter and system module.	18
2.9	Mesh topology of the Neighbourhood Area Network (NAN).	20
2.10	The HAN interface can provide relevant information to devices such as your computer, car, or heater. The objective is to optimize power usage.	21
2.11	The hash value generated by a one-way hash function can be used to validate the integrity of the data sent.	23
2.12	If the same MAC is found, then the message is authentic and integrity is checked.	23
2.13	The symbols used in Yourdon/DeMarco notation	27
2.14	The Data Flow Diagram (DFD) shows the flow of data related to the master meter.	28
2.15	Categories of cyber attack [Per12].	34
2.16	Types of cyber-attacker actions and their motivations when deliberate	36
2.17	Overview of a possible GPRS architecture.	40
2.18	Authentication procedure for General Packet Radio Service (GPRS). The Base Station Subsystem includes the Base Transceiver Station (BST) and Base Station Controller (BSC).	41
2.19	Cryptographic functionality used in Global System for Mobile communications (GSM) and GPRS.	42

2.20	UMTS Authentication and Key Agreement (UMTS-AKA) protocol [Mar16].	44
2.21	Overview of the Universal Mobile Telecommunications System (UMTS) infrastructure.	48
2.22	Phase 1 - Attacker obtains a valid AUTN and RAND.	49
2.23	Phase 2 - Attacker impersonated a valid GSM base station to the victim and selects no encryption.	49
3.1	Encryption in the communication chain for Aidon AMI.	51
3.2	Encapsulation of the Application layer in RF NAN.	54
3.3	MAC-then-encrypt with CRC16.	58
3.4	Encrypt-then-MAC. Note that different keys should be used as input for the encryption algorithm and hash function.	58
3.5	Overview of the meter authenticates to the HES using the RADIUS protocol.	60
3.6	Remote Authentication Dial-In User Service (RADIUS) authentication.	61
3.7	Successful RADIUS authentication in Aidon AMI.	61
3.8	A summary of the RADIUS packet [CR00].	63
3.9	The indicated screws are used to attach the terminal sealing on the smart meter.	64
3.10	Smart meter with the terminal sealing removed.	65
3.11	Smart meter with terminal sealing and interface protection removed.	66
3.12	The red circles outline the metering unit's screws used to hold the front cover. They are covered in plastic stickers which have been removed in this picture.	67
3.13	The internal components of the meter device. 1) Micro controller unit; 2) Multifunction Energy Metering Integrated Circuit; 3) 10 pin connection for communication module.	68
3.14	Communication module used for the meter device. The red circle outlines the SIM card tray slot.	69
3.15	Graphical risk matrix employed in this report.	72
3.16	Mapping of identified business risks.	75
3.17	Mapping of identified technical risks to the risk matrix in Figure 3.15.	77
4.1	M-Bus converter.	81
4.2	The blue cable connects to PIN1 and the red cable connects to PIN2 on the HAN interface.	82
4.3	Overview of the M-Bus converter connected to the meter device.	82
4.4	Configuration of the data channel for the HAN interface.	83
4.5	Serial number of the master meter used for testing.	85
4.6	Slave meter with power strip installed.	87
4.7	Serial number of the slave meter used for testing.	87
4.8	Completed upload of 54,5 kB file to the HAN interface.	90

4.9	Completed upload of 16 byte file to the HAN interface. Note that it says 0.0 Kbytes transferred because of the small file size.	90
4.10	Attempted login using the HAN interface.	91
4.11	Layout of the 4-pin connector on the smart meter.	92
4.12	Layout of the RS232 serial port head [Gro01].	92
4.13	RS232 cable used to connect with the smart meter.	93
4.14	Configuration of the data channel for the RS232 interface	94
4.15	Consumption data from the RS232 reading	96
4.16	Completed upload of 54,5 Kb file to the RS232 interface.	97
4.17	Attempted login using the RS232 interface	97
4.18	First packet capture from the master meter using 10.100.100.1 as IP for the interface.	100
4.19	Second packet capture from the master meter using 10.100.184.1 and 10.100.184.169 as IP for the interface.	103
4.20	Third packet capture from the master meter using 10.100.184.1 and 10.100.184.169 as IP for the interface. Netcat is used to listen for traffic on port 4002 and establish a TCP connection.	103
4.21	Nmap is used to scan for open ports on the meter. Only port 9999 is confirmed open after the test.	105
4.22	Analysis of network traffic in Wireshark when sending data to the meter.	105

List of Tables

2.1	Aidon module types.	17
2.2	List of communication interfaces on system module.	17
2.3	Interfaces on the smart meter [TJL13].	26
2.4	Threats to AMI.	32
2.5	Assets and associated attack goals.	36
2.6	Elements used in the GSM-AKA protocol.	42
2.7	Elements used in the UMTS-AKA protocol.	45
3.1	The table describes an example of a binary data packet that is sent with a fixed interval from the HAN interface.	53
3.2	Business assets for grid companies.	71
3.3	Business Risk Table.	74
3.4	Technical risk table.	76
3.5	Testing plan.	78
4.1	Data analyzed from master meter without load.	86
4.2	Data analyzed from slave meter without load.	88
4.3	Data analyzed from slave meter with load.	89

Chapter 1

Introduction

1.1 Motivation

Norway has great potential for hydropower due to the topology and climate in the country. This has been utilized during the electrification of the country which started at the end of the 19th-century [Joh15]. The expansion of hydropower facilities and grid infrastructure built the foundation for power supply to both the industry and private households [Hof17]. However, technological advancements and population growth have led to increasing power demands [Sta17], and the government acknowledges the need for reconstruction and expansion of the capacity [oe12]. Large investments have been made in the power grid to accommodate the power demands while maintaining supply reliability. In 2016, Statnett invested NOK 5.4 billion in network installations, built 157 kilometers of new power lines, and put into operation 14 new rebuilt power stations. For the next five years, they intend to invest another 35-40 billion NOK [Sta17]. Although the capacity of the power grid will increase as a result of the investments, there will still be periods of limitations in various places on the grid. Statnett gives the following reasons for this [Sta17]:

- Parts of the grid will still be relatively weak, although upgrades are being made.
- The investment plan for coming years contains few measures to increase the capacity between price areas. ¹
- The power consumption in Norway varies greatly depending on the outdoor temperature, and production varies depending on the weather. This gives variations in the power flow and short-term limitations.

¹A price area is a zone where electricity is traded at the same spot price on a power exchange. The area is decided by the transmission system operator and is usually a whole country, or parts of it.

2 1. INTRODUCTION

- Expansion, maintenance, and unforeseen events reduce the capacity and increase the probability of bottlenecks in the grid.

The requirements for reliable power supply is increasing and pushes Norway to develop local solutions as a backup to the grid. Local solutions are closer to the customer, often in the regional grid. Local solutions could be the use of solar panels or installation of smart meters, both at the premises of customers. Smart meters make it easier to integrate local power production with the house and the electrical grid. Advancements in technology have created new opportunities not seen before. There are two fields which make local solutions easier to create:

- Digitization of the energy sector.
- Distributed production and storage of power becomes cheaper.

Digitization of the energy sector enables smarter power consumption and management of the grid. Distributed production and storage could relieve the strain on today's power grid and help with power outages. In December 2017, Tesla built a large battery in South Australia to work as a backup power system. So far it has proven highly effective [Fun17].

The government wants to facilitate the development of new technologies and market solutions to strengthen the reliability of national power supply [Reg15]. One of the more recent upgrades is the introduction of Advanced Metering Infrastructure (AMI). AMI allows for active two-way communication between customers and the Distribution Network Operators (DSOs), where both information and electricity can be exchanged. With detailed consumption data from customers, the power companies can have variable pricing based on the load on the power grid. By presenting end-users with information about their power consumption, they are given an incentive to adjust their usage if DSOs use variable pricing. The goal is to optimize how customers consume and produce power. Moreover, it is in line with the focus on green renewable energy. Local production of renewable electrical power can be integrated with the AMI, making it possible for end-users to produce and sell excess power to nearby households. The infrastructure we have today is built for centralized production and transmission, and passive distribution. A solution where households can produce and trade electrical power with each other, while still using the original power grid, could further reduce capacity problems on the grid [Kjø11].

It has been decided that as of January 1st, 2019, every household in Norway will have a smart meter installed in their home [oe11]. This will hopefully resolve some of the current capacity and supply reliability issues with the traditional power grid.

It will also enable better management of the power grid. Today, the functionality of the smart meter is as follows:

- Automatically reading the customers' power consumption and reporting it to the DSO.
- Power failures are automatically notified to the DSO and can be repaired faster.
- New smart meters add additional features which make management of power consumption for customers easier.

The challenge with introducing the AMI is that by deploying new technology in the power grid, we increase the potential attack surface of it. An attacker could physically compromise a smart meter, or exploit vulnerabilities in the communication to and from the meter. The intention of the attack may be to manipulate the smart meter or other parts of the AMI system for his or her gain.

1.2 Statement of the problem

Norwegian regulations oblige the DSOs to secure their AMI solution, to operate in the Norwegian market [oe14]. Norwegian Electrotechnical Committee (NEK) has made a set of guidelines for how to fulfill the security requirements to meet the regulations. However, it is the DSO who is responsible for the security implementation in their own AMI solution [NVE17]. The only requirement is that they meet the control objectives from The Norwegian Water Resources and Energy Directorate (NVE). There can, therefore, be various implementations of security in smart meters used by different DSOs.

The goal of this thesis is to assess the security of communication interfaces on smart meters. Given the scope of the thesis, we will explore the following research question: *Are there security vulnerabilities in the communication interfaces on smart meters?* Security is a field in constant change, with new vulnerabilities being discovered continuously. Evaluating the security of smart meters given updated knowledge is essential to new threats.

1.3 Methodology

This thesis includes security testing of a smart meter to answer the research question better. The methodology used for this thesis is to first conduct a literature review on security in AMI and smart meters. The literature review gives insight on relevant work that has been done in the field of cybersecurity with regards to AMI and

smart meters. Secondly, it is used to get an overview of the technology used in the meter device tested, focusing on technology for communication. Based on the literature review, we can create a threat model for the smart meter to identify security threats that might be present in its communication interfaces. Next, we will perform an analysis of the meter specifications and a physical inspection of the internal components of the device. With extensive knowledge of the technology used in the smart meter and an understanding of possible threats from the threat model, we can identify areas of interest to test for vulnerabilities. A risk analysis is conducted to discover vulnerabilities in the smart meter, and to estimate the associated risk for DSOs and customers. The risk analysis includes a test plan for vulnerabilities we will test. The test will either strengthen or weaken the suspicion of a vulnerability, possibly confirm if a vulnerability exists.

The methodology used in this thesis requires a comprehensive understanding of the technology used in the AMI and smart meter. Hence, the background, literature and analysis chapters are quite extensive.

To summarize the methodology:

- Literature review: Read about relevant work on security in AMI and smart meters and on the technology used by the Aidon smart meter. Use the information create a threat model for the smart meter.
- Analysis: Obtain detailed information about the security in the Aidon smart meter through a documentation review and a physical review. The physical review includes a physical inspection of the internal components of the meter and identifying potential vulnerabilities for those. Conduct a risk analysis that gives an indication of what vulnerabilities to test. The risk analysis includes a test plan for vulnerabilities. Each vulnerability is evaluated and rated on probability and impact.
- Testing: Test vulnerabilities from the test plan.
- Discussion: Comment on the results, explain what the results mean, interprets the results in a wider context, indicate which results were expected or unexpected, and provide explanations for unexpected results.
- Conclusion: Form a conclusion to the research question based on the literature review and results from the testing.

The separation of information gathering, vulnerability identification, and testing provide a clear understanding of:

- What communication interfaces are on the smart meter?
- How and why are they implemented?
- What vulnerabilities have others discovered on similar technology?
- What potential vulnerabilities are present in the smart meter?
- Is it possible to exploit the vulnerabilities?

1.4 Limitations

The testing in the security analysis is limited to a single smart meter. The meter tested is one that Norwegian University of Science and Technology (NTNU) has received from Aidon. It does not meet the same security requirements needed to be installed at a customer. Aidon is one of the major producers of smart meters for the Norwegian market. The work is therefore relevant with regards to the deployment of smart meters in Norway.

We will not perform any destructive testing. Furthermore, we will not do any physical modifications to the smart meter. The testing will focus on vulnerabilities in the communication interfaces of the smart meter. Testing of the Head End System (HES) is excluded since we do not have hardware or software to replicate the HES functionality.

Some information about the AMI solution provided by Aidon will not be included because it is considered confidential and sensitive.

1.5 Thesis structure

Chapter 2 explains how the electric system in Norway works, what smart grids are, details surrounding the AMI solution provided by Aidon, and a threat model of the AMI. Also, it presents useful research that has already been done about security in smart meters, or technology used by the smart meter. Chapter 3 analyzes the security in the Aidon smart meter and AMI. It also includes a risk analysis used for testing. Chapter 4 includes the tests and results of some identified and prioritized vulnerabilities. Chapter 5 includes a discussion of the results from the testing. Chapter 6 concludes the thesis.

Chapter 2

Literature review

This chapter introduces general terms and concepts regarding the electrical grid, smart grid, and Advanced Metering Infrastructure (AMI). Secondly, it portrays the security and threat landscape of one actual AMI and smart meter. At last, we introduce relevant writings about mobile communication technologies in smart meters. We did not come across any publications that include practical testing of smart meters or AMIs. The lack of publications is most likely because such work is confidential. There exists a Python framework for security testing of smart meters, called Termineter. However, the framework only supports meters using the C1219-2007 protocol with 7-bit character sets. This configuration is the most common for smart meters in North-America [McI18]. Aidon does not use this configuration for their smart meters, and we will therefore not look at the framework in this thesis. Several articles about the security of smart meters focus on vulnerabilities in the wireless communication technology used between the meter and Head End System (HES) [Her16] [Kov17]. We will include a security review of the wireless technologies 2G and 3G. A review of 4G is not included, as 2G and 3G are considered most insecure. However, 4G technologies such as LTE is vulnerable to some attacks [MO17] [Oli17].

2.1 Electrical grid

The Norwegian Government has stated that a secure and reliable power supply is essential in any modern society [oe12]. It is, therefore, important for Norway to have a well-functioning power system with a reliable supply of electricity since almost all important public services and functions are critically dependant on it. Electricity is also heavily incorporated into the industry and the everyday lives of people. In this section, we will cover the electrical grid and electricity market in Norway.

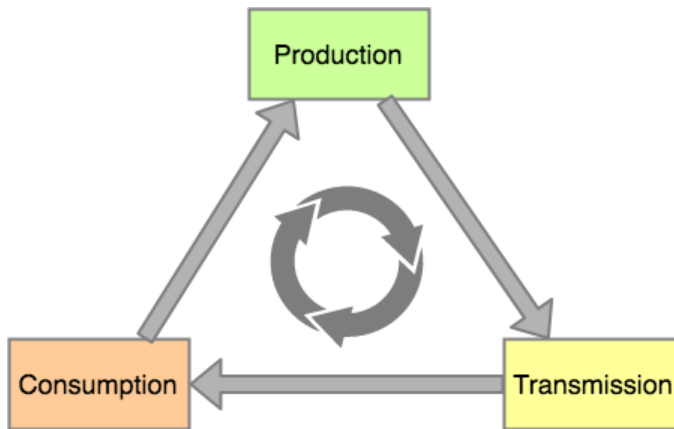


Figure 2.1: The life cycle of electricity can be separated into three stages: production, transmission, and consumption.

2.1.1 Grid infrastructure

The distance between production and consumption of electricity is most often long. The electrical grid is built with the purpose of transporting electricity from the production plants to the end users. It consists of some core components which are power plants, transformers, transmission lines, and distribution lines. The components are used in different parts of the electric life cycle. The life cycle of electric power can be divided into three stages: production, transportation, and consumption. Figure 2.1 First, the power is produced at a power plant that creates electricity from an energy source. In Norway, the energy source is mainly hydropower. Then, the power is transported through highly conducting wires installed on towers or poles. Finally, the power is consumed at the end user. The consumption of electricity affects how much electrical power is produced, making the life cycle continuous.

High voltage is required when transporting electricity across long distances. However, the facilities to manage high voltage electricity are expensive. Therefore, today's infrastructure follows a hierarchical topology where the relationship between voltage and the number of connections to the grid is reverse proportional (see Figure 2.2). There are less high voltage connections and more low voltage connections.

Figure 2.3 illustrates the five stages of the supply of electricity in Norway. First, power is produced at power generating facilities. Then, it is transported using the main grid, regional grid, and distribution grid. It is then consumed at the end user. We will now explain each step.

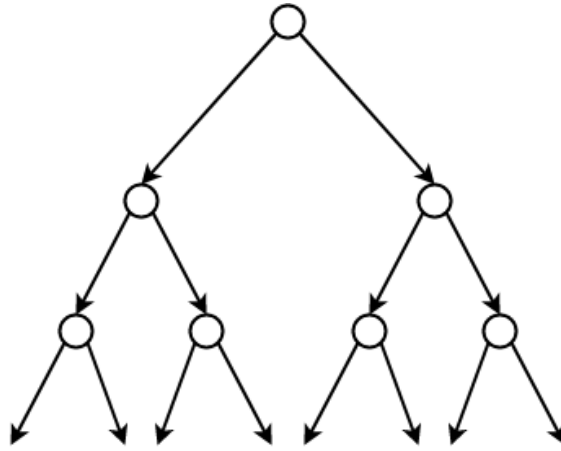


Figure 2.2: The hierarchical topology of the electric grid is reverse proportional, and can be compared to a tree graph.

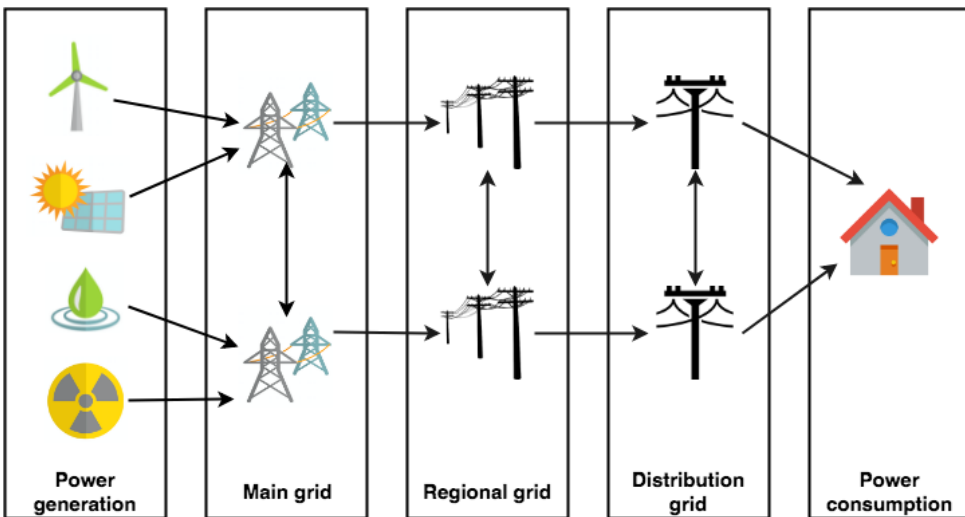


Figure 2.3: The supply of electricity can be separated into five stages.

Power generation Electric power is generated at power generation plants. Different power generation plants can be hydroelectric stations, wind power installations, fossil fuel plants, thermal power plants, and nuclear reactors. The plants can be publicly owned or owned by private organizations [Ros17]. It is common that they produce several hundred megawatts. The electric grid must always be in equilibrium. That is, the consumption of electricity must be equal to the amount produced or imported [Nor17b]. The balance between consumption and production is called the instantaneous balance. Failing to maintain the instantaneous balance in the electric grid may in the worst case lead to damage to components in the infrastructure or power outage.

Main grid The main grid is used to transport electricity from the power plants across long distances to regions. It connects larger producers and consumers in a nationwide system. The main grid also includes transborder connections to other countries. Before the electric power is sent, it is stepped up to a higher voltage, usually between 300 kV and 420 kV [oe17]. In Norway, we have a single Transmission System Operator (TSO) named Statnett, which operates the main grid [Sta14].

Regional grid When the electric power from the main grid reaches a destination region, the voltage is stepped down to a level between 33 kV and 132 kV [oe17]. The regional grid is used to transport electric power to demand centers where the end users are, and connect the main grid and the distribution grid. Production of electric energy may happen at the regional grid level. The regional grid is owned by Distribution Network Operators (DSOs), such as Hafslund, BKK and Lyse Energi, but is heavily regulated by the state.

Distribution grid Once the electric power has reached a demand center, it enters the distribution grid. From here, the power is transported to the end users, including households and industries. The voltage levels in distribution grids vary around 230V to 22 kV and are therefore separated into a low- and high-voltage distribution grid. Transformers are used to transform the power to 230V before it enters a household. 230V is the standard voltage in Norway and most countries in Europe. Industries often require electricity with higher voltage and can choose not to step down the voltage, or transform it to a specified voltage. Industries can, therefore, be connected to the high-voltage or low-voltage distribution grid, while households are only connected to the low-voltage distribution grid.

Power consumption Electrical power is consumed by end users, which can be households and industries. The total power consumption in a country is given by

equation 2.1.

$$Consumption = Production + Import - Export \quad (2.1)$$

2.1.2 Organization of the electrical grid

Statnett owns the majority of the main grid in Norway and is the system administrator of the Norwegian power system. It is a state enterprise, meaning that the Norwegian state wholly owns them. The Ministry of Petroleum and Energy represents the organization. Regional DSOs own roughly six percent of the main grid [Nor17a].

Municipalities and county authorities own most of the regional and distribution grids, but there is also some amount of private ownership [Nor17a].

Many DSOs are part of integrated companies. Integrated companies have their business operations across the whole supply chain of a business. In the electrical power business, this includes operations in power production, power transmission, and power trading. The Norwegian Parliament introduces a new legislative decision in 2021, requiring all integrated DSOs to conduct a corporate and functional separation [oe16]. The goal of the legislative decision is to separate the market and monopoly in the electrical power market more clearly [Nor17b].

2.1.3 Electricity market

Trading electricity is done in mainly two markets, the wholesale market and the retail market. This is illustrated in Figure 2.4

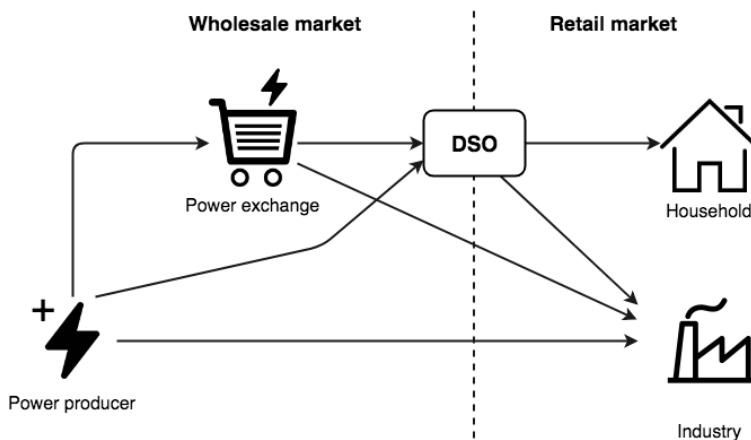


Figure 2.4: Overview of the energy market.

Wholesale market

The wholesale market enables power producers, suppliers, larger industrial enterprises or other participants to buy and sell power in competition with other market participants in the electricity wholesale market. The wholesale market also facilitates import and export of power to Norway.

Norway is part of a joint power market for Nordic and Baltic countries, called Nord Pool. Nord Pool is an organization which facilitates trading, clearing, settlement and associated services in both day-ahead and intraday markets across the countries. National TSOs in Nordic and Baltic countries own Nord Pool. The market price of power at the Nord Pool exchange is determined each day and is a result of supply and demand between the countries. Furthermore, the Nord Pool market is integrated into the European power market through interconnectors to Germany, Netherlands, Estonia, Poland, and Russia. The coupling of markets ensures that electricity flows following market prices, thus ensuring optimal use of capacity and production resources [oe18]. Norway has a significant share of flexible hydropower. In periods with favorable hydrological conditions, production is high, but national power consumption may be low. Norway can then export excess power to countries at a better price in times of oversupply.

Retail market

The retail market includes all households and business consumers that purchase electricity from a retailer or a broker. The end user has to pay a monthly grid tariff to the DSO, in addition to consumed electricity. There are many DSOs with different price models and contract conditions. The DSO can purchase power on the international power market, e.g., Nord Pool, and sell it to the end users. In some places, the DSO and power producer are the same company (integrated). All DSOs have a monopoly within a given geographical area. The reason for having a monopoly is that it would be unprofitable for DSOs to build parallel transmission lines. The terms for operating in a monopoly are that the DSOs are obliged to deliver grid services and follow regulations set by The Norwegian Water Resources and Energy Directorate (NVE).

2.2 Smart grid

This section will describe what the smart grid is, briefly how it works, goals and challenges that it tries to solve. Note that all numbers presented in this section are from electricity grids in the USA. Although they do not apply directly to the electricity grid in Norway, they provide good insight on some of the issues with the traditional grid infrastructure.

The former electricity grid is unidirectional, meaning that information and power only flow in one direction on the grid. Almost 8% energy is wasted as heat along the transmission lines, and 20% of generation capacity exists to meet peak demand only [Far10]. The hierarchical nature of the grid infrastructure makes it vulnerable to domino-effect failures. That is, failures closer to the power plants will have a more significant impact on the end users. It is estimated that nearly 90% of all power outages and disturbances have their roots in the distribution network [Far10]. The smart grid is expected to solve all of the challenges with the former traditional power grid.

The smart grid allows for active two-way communication between customers and the DSOs, where both information and electricity can be exchanged. The goal is to optimize how we consume and produce power by utilizing more detailed consumption data. The smart grid introduces distributed measurement and management systems, new sensor technology, and remote management of equipment [Kjø11]. The new functionality will provide DSOs with better visibility and control over their assets and services. Furthermore, it is expected to make the grid more resilient by having a proactive response to anomalies or other faults. At last, the smart grid enables new ways of engaging with each other and performing energy transactions across the system. Figure 2.5 illustrates how the smart grid interconnect more elements in the power grid.

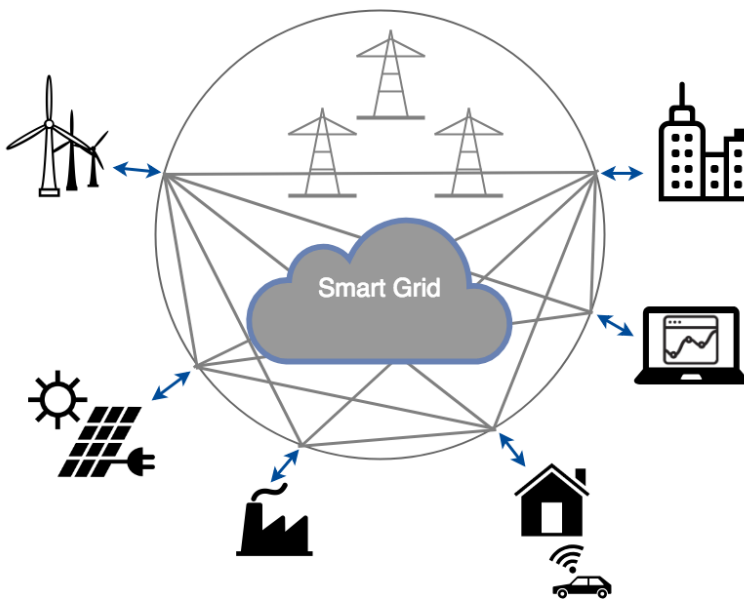


Figure 2.5: The smart grid will interconnect more elements in the power grid, moving away from the traditional hierarchical topology.

To enable the applications of the smart grid, we need to install a layer of intelligence in the power grid, which requires new infrastructure. Given the size and value of the existing grid infrastructure, the implementation of new infrastructure will most likely have an evolutionary trajectory. DSOs have already invested heavily in utility assets, and want to ensure that they achieve the highest possible return on the required investments for the smart grid. A drastic overhaul is not desirable as it will be a significant expense and possibly jeopardize the services they are currently providing.

Nearly 90% of all power outages and faults happen in the distribution network [Far10], making it the most prominent part of the power grid to upgrade. The AMI is one of the initiatives made to bring Norway closer towards a smart grid.

2.3 Advanced Metering Infrastructure

This section will discuss the purpose of AMI, the architecture and components, and the topology. Since the scope of the thesis is on communication interfaces of the smart meter, we will explain this technology more in-depth. Some relevant protocols and standards will be outlined as well.

2.3.1 Purpose of AMI

The AMI is a term used to describe a system which measures, collects and analyzes data about energy consumption from smart meters. Components of the AMI are both hardware and software.

As previously discussed, AMS allows two-way communication between the DSO and the end-users. This enables the DSOs to send commands to the smart meters, and for the end-users to frequently report their power usage back. The extent of the functionality is not fully explored, but some commands from the DSO can be:

- Time-based pricing information.
- Demand response actions. That is, actions to maintain the instantaneous balance in the grid.
- Remote service disconnect.

Time-based pricing information is used to accommodate periods of high load on the power grid. By obtaining information about when the load is high, the DSO can use time-based pricing as an incentive to reduce consumption during periods of high load. As an example, we can look at how people charge their electric cars.

In Norway, it is common to have an eight hour work day which finishes at 4 PM. People drive their electric car from work and start charging it once they arrive home. If many people start charging their car at the same time after work, it is going to strain the capacity of the power grid. The DSO could then adjust the pricing of electricity to be more expensive between, e.g., 4 and 7 PM. This would encourage more people to charge their cars during the night, for example, reducing the peak load on the grid. Time-based pricing is an example of demand response action. Demand response is used to match the demand for power with the supply better. As previously mentioned, the power grid needs to be in instantaneous balance. This can be done in two ways, import and export of electrical power, or adjusting production of electrical power to the demand. However, it is not always desirable to export or import power for various reasons. Furthermore, power generating units can take a long time to come up to full power. Having end-users to adjust their consumption to the production is, therefore, a measure to keep the instantaneous balance.

Remote service disconnect is the ability for the DSO to remotely disconnect a user from the power grid, or throttle their consumption. There are various reasons for this functionality. For example, if they do not pay their electric bills.

2.3.2 Architecture and components

The architecture used in Aidon's AMI solution consists of three main components: HES, smart meters, and communication lines. This is illustrated in Figure 2.6.

Head End System

The HES is located in the network of the DSO. It communicates directly with the smart meters and is responsible for collecting data from end-users and sending commands. The HES enables the DSO to manage and operate the grid more efficiently. The HES consists of different application servers, database servers, systems, and workstations. Collected data from end-users is managed using a Metering Data Management (MDM) system.

Smart meter

The smart meter is responsible for measuring power consumption in households and report it to the HES. It also provides the end-user with useful information about their consumption. There are two types of smart meters, slaves, and masters:

- **Master:** The master meter works as a collector or gateway for data from other meters, which it relays to the HES. All communication between the slave meters and HES is redirected through the master. Depending on the infrastructure, the master can function as a meter itself while being a collector.

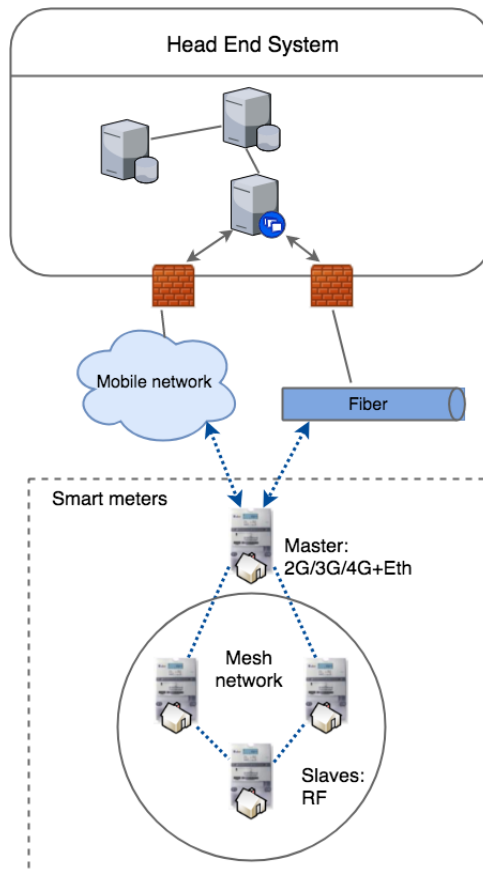


Figure 2.6: Overview of the AMI.

Each neighborhood has a master. It communicates directly with the HES using either the mobile communication or fiber optic communication (Ethernet).

- **Slave:** The slave meter is installed on consumer premises. Slave meters are organized in a mesh network using Radio Frequency (RF). In this way, they can either communicate directly with the master or work as a relay to route data between other slave meters and the master.

The smart meter is modular, and have a system module installed. The system module provides communication interfaces to facilitate communication between meter devices and to the HES. The system module can also extend the energy metering functionality to tasks such as the provision of time-stamped registry values, control of loads, monitoring of power quality, registration of power outages and fault

Module	Type	Uplink comm.	Master – slave communication	Recommended usage
Aidon 6475 Aidon 6476	RF2 Master	2G/3G/4G	Local radio 500 mW	Used to measure public facilities such as street lights and transformer stations. Located on points with easy access and wide radio coverage.
Aidon 6477 Aidon 6478	RF2 Master	2G/3G/4G Ethernet	Local radio 500 mW	Used to measure public facilities such as street lights and transformer stations. Located on points with easy access and wide radio coverage.
Aidon 6483 Aidon 6484	RF2 Slave	-	Local radio 500 mW	Used to measure power consumption of single households in urban or rural residential areas.

Table 2.1: Aidon module types.

#	Interface of Slave and Master	#	Interface only on Master
1	RS-232 connector or HAN adapter connector for +24 V M-Bus	4	External antenna connector (uplink 2G/3G/4G)
2	2 status connections	5	RJ-45 connector (uplink LAN/Ethernet)
3	External antenna connector (local Aidon RF2)	6	SIM card slot (micro)

Table 2.2: List of communication interfaces on system module.

information, as well as the reading of external status information [Aid17b]. The benefit of a modular smart meter is that the meter and system module can have a different lifespan.

Module types Table 2.1 provides basic information about the Aidon system modules.

Interfaces on system module The system module is installed on the right side of the smart meter. The communication interfaces on the system module are different between the slave and master unit. This is because the master meter needs communication interfaces which facilitates communication with the HES. Figure 2.7 shows the interfaces on the Aidon 6478 system module tested in this thesis.

Meter architecture The architecture of the meter and the system module is illustrated in Figure 2.8.

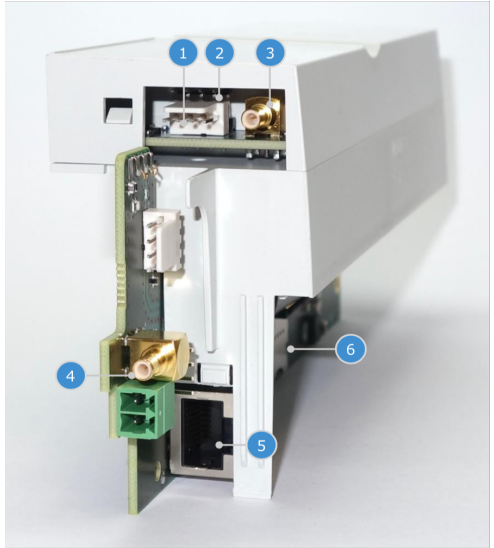


Figure 2.7: The system module has several connection interfaces depending on the model.

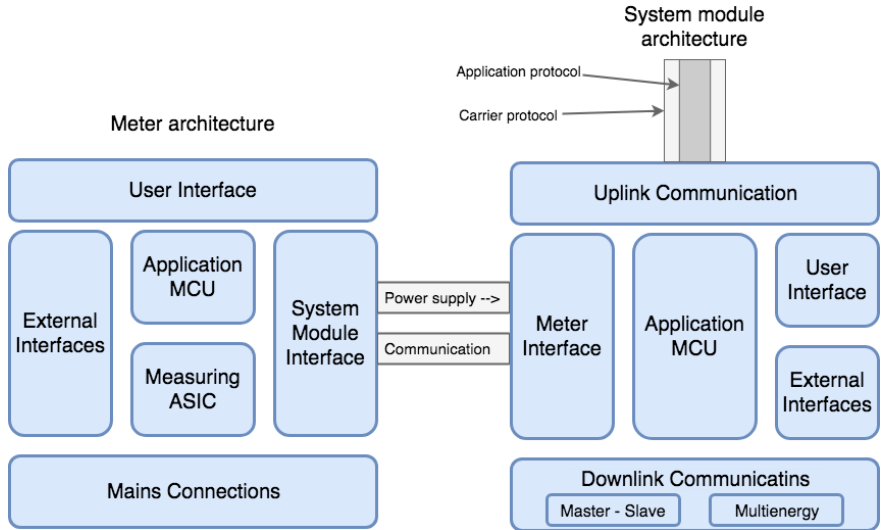


Figure 2.8: Overview of the internal architecture of Aidon's 6000 series meter and system module.

2.3.3 Communication

Data is transmitted across three types of networks in the AMI infrastructure. These networks are the WAN, NAN, and HAN.

Wide Area Network

The WAN connects the smart meters to the HES. Communication on the WAN is Internet Protocol (IP) based. It relies on infrastructures such as Fiber Optic Cables (FOC), 2G, 3G, and 4G. 2G, 3G, and 4G are not technologies but refers to a generation of wireless technologies. Each generation has standards that technology must fulfill to use the correct G terminology.

Neighbourhood Area Network

The Neighbourhood Area Network (NAN) connects the smart meters, including slaves and masters. The devices form a mesh network, and the slaves send data to the master meter, either directly or through a relay of other slaves. Figure 2.9 illustrates the mesh topology of the NAN. A mesh topology provides resiliency in the network. If one of the smart meters breaks down, other meters relays the traffic to the master. Communication is based on the radio signal and is defined by the Short-range Device (SRD) ETSI standard [Aid17a]. The smart meters utilize a license-free European frequency band between 868.000-875.600 MHz, divided into multiple channels.

The maximum number of slaves per master is 1000. However, Aidon recommends somewhere between 20 and 500 slaves per master. There should be at least two other meter devices within a 600-meter radius from each device in the RF NAN, to ensure reliable and stable communication to the HES.

Home Area Network

The smart meters installed in households collect data about the power consumption. This data is available to external devices through the Home Area Network (HAN) interface as displayed in Figure 2.10. For example, the customer could connect a display to the HAN interface and get information about consumption. Few companies are providing services related to the HAN interface so far. It is likely that customers will connect the smart meter to their private Local Area Network (LAN) to quickly access the data from multiple devices. Such solutions are already in development [Acc17].

The HAN interface on the Aidon 6478 system module has two pins:

- **RJ-45 PIN1:** +24V M-Bus (Line 2 from internal interface)

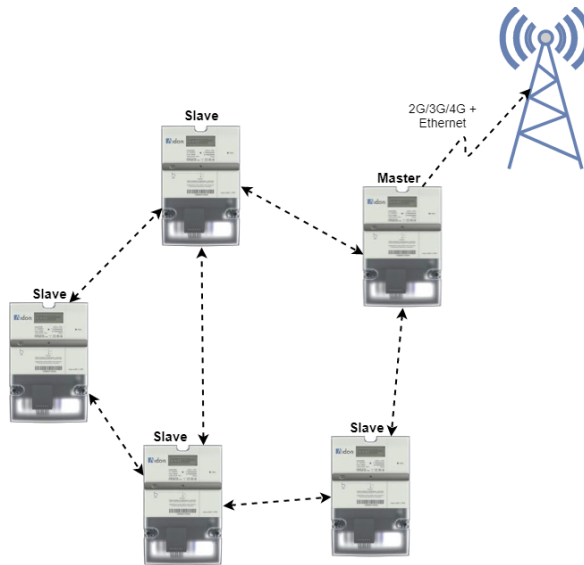


Figure 2.9: Mesh topology of the NAN.

- **RJ-45 PIN2:** GND (Line 1 from internal interface)

The following protocols are used for communication on the HAN interface for all system modules:

- **EN 62056-7-5:** Local data transmission profiles for Local Networks (LN)
- **EN 13757-2:** M-Bus physical layer
- **EN 62056-61:** OBIS codes
- **EN 62056-62:** Interface classes

EN 62056 is a set of standards for Electricity metering data exchange by the European Committee for Electrotechnical Standardization (CENELEC) [fES15]. The HAN interface is unidirectional by default configuration, according to the EN 62056-7-5 standard proposal. It is designed only to push data from the interface.

2.4 Security in AMI

This section gives a general introduction to information security before presenting a threat model of the AMI. This will help us identify assets and risks related to the

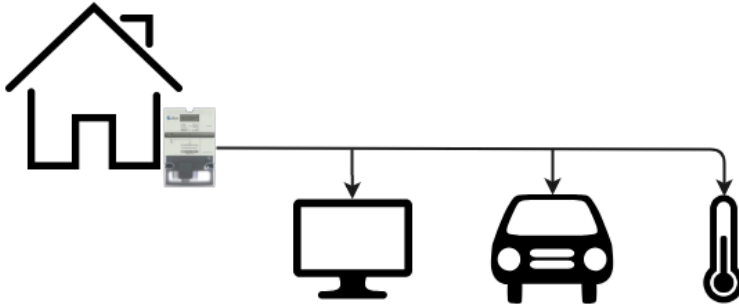


Figure 2.10: The HAN interface can provide relevant information to devices such as your computer, car, or heater. The objective is to optimize power usage.

communication interfaces on the smart meter. We will also look at the motivation for cyber attacks on AMI and smart meters.

2.4.1 Introduction to information security

Information security is the practice of securing assets by preventing a breach of confidentiality, integrity, and availability. These three terms are generally known as the CIA triad. Although the terms might sound simple, they provide great outreach and are adequate to an organization as long as the concepts of CIA are well-maintained [Ins17]. This thesis will use the CIA triad when evaluating security for the communication interfaces. Let us have a closer look at the three terms.

- **Confidentiality:** Information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity:** Data cannot be modified in an unauthorized or undetected manner.
- **Availability:** The service or data on the application must be available to the user when needed.

It is crucial to classify assets and information, and have a secure access policy for these, to support confidentiality. The policy should revolve around the principle of "least privilege" which means that information is only available to some people, not all. For example, not everybody in a company should have access to the same information as the CEO. The company needs a strong data classification policy to ensure correct data policies. Confidentiality is also supported by using encryption on data. Encryption converts plain text into cipher text, making it useless unless the person knows how to decrypt it. Note that it is possible to break the

encryption, but if the encryption algorithm applied to the plaintext is secure, this is considered unfeasible. When considering confidentiality of information sent on the communication interfaces on smart meters, it is highly relevant to look at what encryption algorithm is used.

There are different ways to maintain the integrity of data. For data at rest, meaning data stored in systems or databases, it can be maintained through access controls and the use of accepted procedures to change the data. Another standard technique is to include a hash of the original data when storing or sending information. The hash is calculated by using a one-way hash function. This is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (called the hash). When data is sent, the calculated hash value is added to the message. The recipient can recalculate the hash of the message, given knowledge of the hash function used, and see if it matches the hash value received. If it does not match, the recipient knows that the data has been modified during transmission. Figure 2.11 illustrates how hash can be used for integrity checking. The one-way property of the hash function makes the attacker unable to correlate the input and output of the function. However, the method of adding a hash at the end of the message has a weakness. If the attacker knows which hash algorithm is used, he can recompute a new hash value for a modified message. The message will then look valid with the new hash value. Using hashes is, therefore, only recommended for detecting random errors.

Another option to maintain the integrity of data is to use a Message Authentication Code (MAC). A MAC can be used to check the integrity and authenticity of a message. It is a cryptographic checksum on data which uses three different algorithms:

- Key generation algorithm: Selects a signing key from the key space uniformly at random.
- Key signing algorithm: Returns a MAC given the key and the message.
- Verifying algorithm: Verifies the authenticity of the message given the key and the MAC.

Just like the recently discussed hash value, a MAC is added to the message. The difference is that MACs are produced given a message and secret key as input. The secret key is only known by the sender and recipient. The recipient can check the integrity and authenticity of the message by using the verifying algorithm. Inputs to the verifying algorithm are the message and secret key. It is unfeasible for an attacker to recompute a valid MAC value to the modified message because he does not know the secret key. If the recipient recalculates the MAC for a modified message,

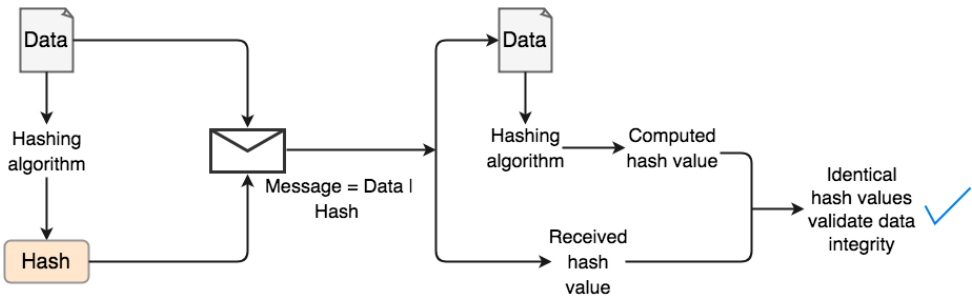


Figure 2.11: The hash value generated by a one-way hash function can be used to validate the integrity of the data sent.

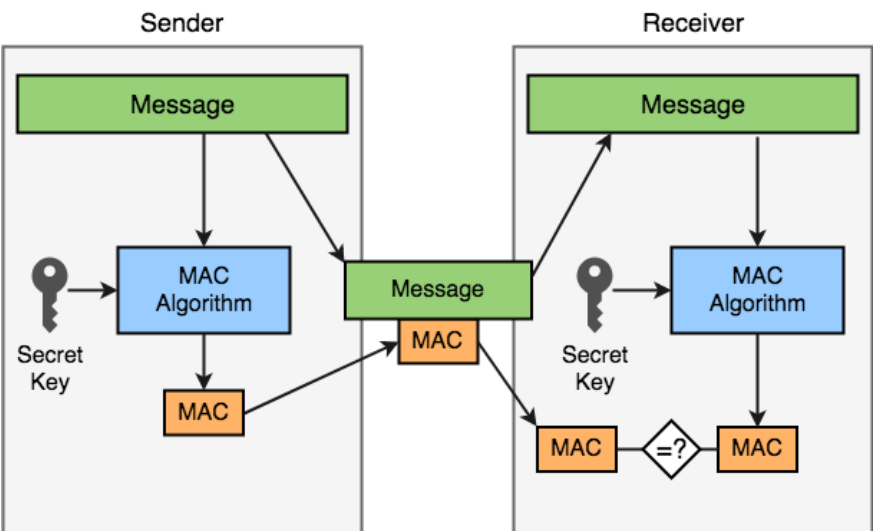


Figure 2.12: If the same MAC is found, then the message is authentic and integrity is checked.

it will not match the MAC received. This is unless the attacker manages to guess the correct MAC. It is recommended to use MACs to check the authenticity of a message and check for random errors or deliberate modifications to a message. Figure 2.12 illustrates how MAC works. There are four types of MACs: unconditionally secure, hash function-based, stream cipher-based and block cipher-based. We will not discuss the different types in this thesis.

Availability can be threatened by cyber attacks, but also by human-made incidents or natural disasters. It can be challenging to achieve high availability, but it is

incredibly desirable for critical systems as downtime can have significant consequences. There are three principals used in systems design to help achieve higher availability.

1. Elimination of single point of failure. This can be done using redundancy in the system, meaning that if one component fails it does not bring down the whole system.
2. Reliable crossover. If a component fails, the system must support reliable crossover to other components to continue to provide the functionality of the system.
3. Detection of failures. Although the user of the system does not see the failure, it must be detected by whoever is responsible for maintaining the system.

An example of elimination of single point of failure is to use a mesh topology in the NAN. If one slave meter goes down, there are multiple others which can be used to relay traffic. One of the critical features of introducing the AMI is better detection of a failure in the system. Lastly, if a fault is detected, it should be automatically reported, and a reliable crossover should occur if possible.

2.4.2 Importance of security

Thanks to companies such as Amazon, Netflix, and Apple, customers are now expecting a quick and seamless digital experience when using a product or service [SM14]. These high customer expectations are spreading to all other industries. Companies must accelerate the digitization of their business processes to meet their expectations. Digitization includes making more processes, information, and resources digital. The digital footprint of the organization increases and so does the risk of cyber attacks. Making processes, information and resources digital create new possible attack vectors. The importance of security has, therefore, become more evident for organizations as businesses are undergoing digitization. The reason is that a successful cyber attack can have a substantial economic impact on an organization, indirectly and directly.

More countries are enforcing data protection laws to prohibit the disclosure or misuse of information about private individuals. Because modern smart meters generate detailed data, both geographically and in time, it is considered personal data [AS17]. In Norway, the Personal Data Act (PDA) §13 obliges sufficient information security when handling personal data [ob01]. The purpose of the law is to protect individuals from having their privacy infringed upon when organizations process personal data. It forces the DSOs to use smart meters which provide adequate security to be compliant with the PDA. Norwegian Electrotechnical Committee

(NEK) provides guidelines for how to implement security in the smart meter. In addition to the PDA, DSOs need to be compliant with the newly introduced data protection and privacy law General Data Protection Law (GDPR). The goal of GDPR is for citizens to regain control over their data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

Given the PDA and GDPR, confidentiality of customer data seems to be the most prominent principle to which providers want to attend. However, it is in the interest for DSOs to maintain integrity and availability as well. Lack of integrity may have financial consequences. Attacks on availability may cause dissatisfied customers, even threaten the security of the country as its infrastructure relies heavily on electricity [Har16]. We will touch more on the consequences of the threats related to the smart meter in the threat model. Sufficient security is not only a matter of being compliant with laws, but about securing the company's assets, maintaining a good relationship with the customers, and maintaining national security. It can be difficult to identify all threats in the AMI since it is the first major digital overhaul of the power industry in Norway. Nevertheless, NEK summarizes the following elements as the most important when looking at security in the smart meter [Kom15]:

- Protection against unauthorized access to meter data.
- Protection against unauthorized extraction of meter data.
- Protection against manipulation of meter data.
- Assurance that the meter data is available on demand.

2.4.3 Threat model of AMI

Threat modeling is a structured way to identify, enumerate, and prioritize threats, presenting all the information that affects the security of the system. A threat model of the AMI helps form an overview of the security on the smart meter, giving us an idea of where to look when testing for vulnerabilities. It enables informed decision-making about risks present in the smart meter.

In this thesis, we will use a lightweight threat model to identify attack vectors on the AMI, and valuable assets for an attacker. The work is based on a previous threat model of the AMI from SINTEF [TJL13]. We will model the flow of information in the system using a Data Flow Diagram (DFD). Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privileges (STRIDE) is used to classify the threats, ensuring coverage of all vulnerabilities [Sho14]. The threats towards the AMI are addressed in two ways:

ID	Where	Interface	Communication
I1	Meter - HES	1) Ethernet 2) 2G/3G/4G	Establishment and maintenance of communication link; Readings and events; Control messages (including software updates, configuration changes, meter reading requests and updated keys); Login management; Status
I2	Meter - Meter	3) RF signal (ETSI standard)	Network management; Readings and events; Control messages; Login management; Status
I3	Meter - Third Party Equipment	4) HAN interface 5) RS232	Meter readings; Reading requests
I4	Meter - Local Maintenance	6) Status input connection	Requests; Credentials; Configuration data; Stored meter data and logs; Test results

Table 2.3: Interfaces on the smart meter [TJL13].

- Threat overview: The interfaces on the master meter are identified, and the flow of information from the interfaces are modeled using DFD. Threats against the interfaces are identified and classified using STRIDE.
- Attacker strategies: Important assets of the system are identified using previous work by SINTEF and analyzing the system. Attack goals are associated with the assets and the motivation of the attacker.

Data flow related to meter

The communication interfaces for the smart meter are all in the system module. It contains a total of six communication interfaces if we exclude the SIM card slot. The interfaces are listed in Table 2.3. The identified interfaces, and information about the AMI infrastructure (see Chapter 2.3), are used for creating the DFD. Slave meters have similar data flows as the master meters, except for the communication with the HES.

There are several symbols used for creating a DFD. However, when using any convention's DFD rules or guidelines, the symbols depict these four components of data flow diagrams:

- **External entity:** External entities are objects outside of the system, which communicate with the system by sending or receiving data. In other words, they are sources and destinations of data in the system.





Notation	Symbol
External entities	
Process	
Data store	
Data flow	

Figure 2.13: The symbols used in Yourdon/DeMarco notation

- **Process:** Transforms data in the system by modifying it or changing its direction. For example, a process can change data using computations, sort the data using logic, or direct it using business rules.
- **Data store:** Files or repositories that hold data in the system. For example a database.
- **Data flow:** Connects components and represents the direction of data. That is the route for data between entities, processes and data stores.

The Yourdon/DeMarco notation is used to create the DFD which represents data related to the master meter (see Figure 2.13). Figure 2.14 shows the DFD diagram.

Threat overview

We will use STRIDE when identifying threats to the AMI. STRIDE is a classification scheme for characterizing known threats to different kinds of exploits. That is, we can use STRIDE to classify threats that have been identified. STRIDE categorizes threats into six different categories:

- Spoofing.
- Tampering.
- Repudiation.
- Information disclosure (privacy breach or data leak).

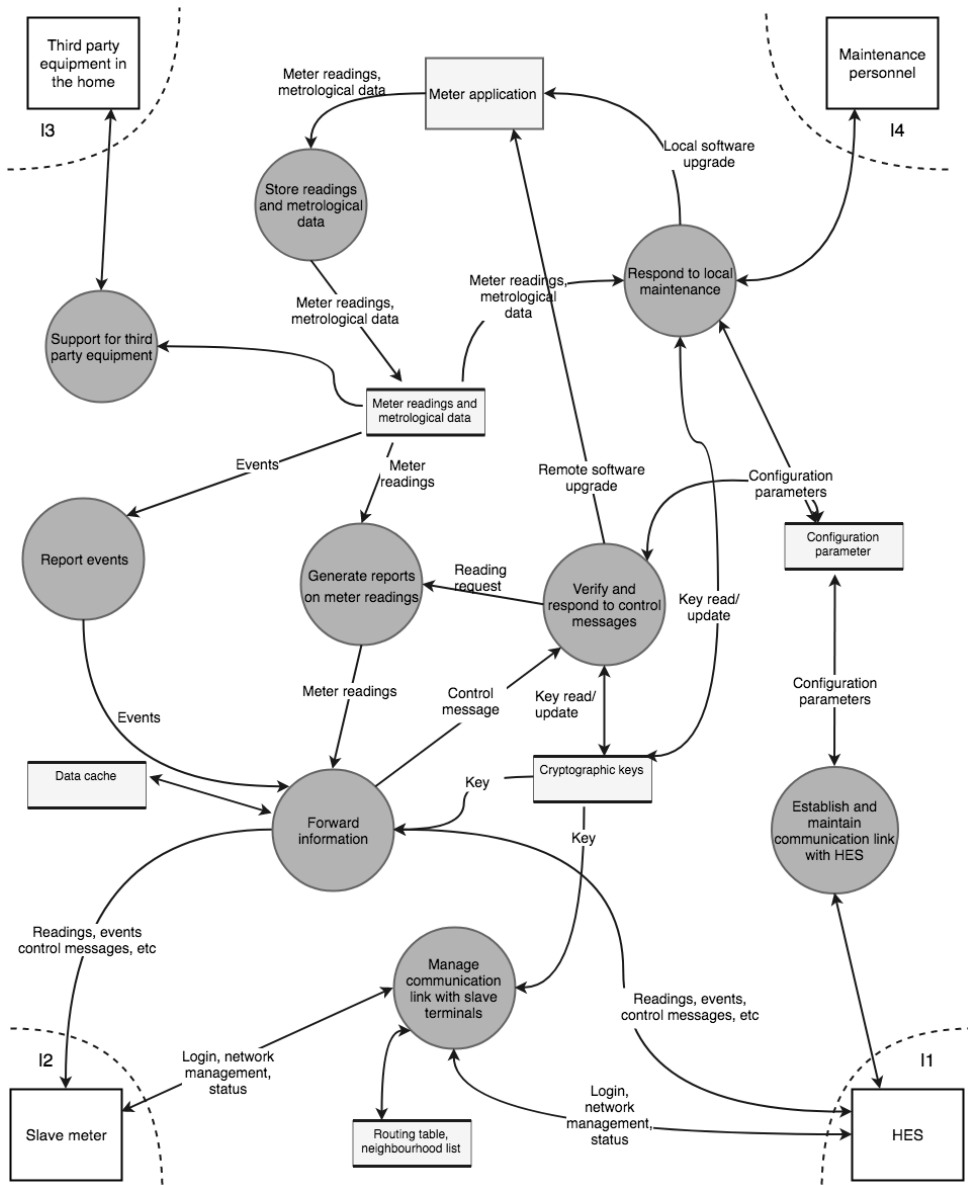


Figure 2.14: The Data Flow Diagram (DFD) shows the flow of data related to the master meter.

- Denial of service.
- Elevation of privilege.

Spoofing: Spoofing is a type of fraudulent activity where an attacker can pose as another user, component or system when communicating with a receiver. An example of spoofing is when a person illegally obtains and uses the authentication information of another user. Interface I1 and I2 are potential targets for spoofing attacks (T1-T3 in Table 2.4). For communication between the master meter and HES, an attacker could spoof the identity of the HES. This could allow him to obtain data from the meters, and send fake commands. Meter spoofing can result in access to data from other meters. Furthermore, it could be possible to generate false meter reports. Commands from the HES could potentially be intercepted and dropped if the attacker poses as a master meter. There is no use of identities on the HAN and spoofing on the I3 interface is not considered relevant. I4 requires physical access, making it hard to spoof. However, the possibility of spoofing the maintenance personnel should be considered (T4).

Vulnerabilities towards spoofing in AMI depend on how well authentication mechanisms are implemented, what the procedures for contact establishment are and the existence of spoofing detection mechanisms.

Tampering: Tampering is the same as an unauthorized modification of data, which is a breach of integrity. Lack of integrity is a threat to the AMI because it relies on accurate data to provide services such as billing. There are two communication interfaces on the master meter that looks prone to tampering attacks. These are interface I1 for communication with the HES, and interface I2 for communication with other meters. An attacker could potentially perform a Man-in-the-middle (MITM) attack to intercept and modify data (T5-T7 in Table 2.4). Tampering of data on I1 and I2 could result in errors in meter reading reports, wrong configuration settings, unauthorized changes of software, or erroneous or missing alarms [TJL13]. For interface I4, tampering can happen, either by local maintenance personnel altering meter data or by the meter reporting wrong data to local maintenance (T8-T9 in Table 2.4) [TJL13]. For interface I3, an attacker could use third-party equipment to alter meter data or software on the master meter (T10).

The vulnerabilities towards threats T5-T7 depend on the security of the communication infrastructure and protocols used in AMI. For example, 2G technology for communication to the HES provides no mutual authentication between the smart meter and cell tower, which is a potential weakness. The security also relies on the strength of any integrity protection. Threat T8 depends on the vulnerability towards T4 (Attacker is authenticated as maintenance personnel) and the system's ability to

detect unauthorized changes. Threat T9 depends on the feasibility of compromising a meter. If it is relatively easy, then T9 is more likely to occur. Threat T10 depends on the communication protocols used for communicating with third-party equipment. If the meter accepts unauthorized data, then this can pose a threat.

Repudiation: Repudiation threats allow adversaries to deny any malicious activity they have performed because the system does not have sufficient auditing or record keeping of their activity to prove otherwise. Non-repudiation should be implemented to provide proof of the integrity and origin of data, and to provide valid authentication with high assurance. Non-repudiation is essential for the AMI and its financial transactions, metrology information, and responses to control commands. On interface I1 and I2, meters could deny receiving or sending messages (T11 and T12 in Table 2.4). On interface I3, the meter could deny sending harmful information to third-party equipment. On interface I4, either the maintenance personnel or the meter could deny the maintenance (T13).

The system needs to be able to prove the origin of messages, and maintain integrity protection of messages, to prevent T11 and T12. For threat T13, logging functionality should be implemented on the meter or by the maintenance personnel, as well as protection for the audit logs.

Information Disclosure: Information disclosure is *the exposure of protected data to a user who is not otherwise allowed access to that data* [SS04]. Data transmitted on the communication interfaces of the smart meter includes private consumption data, encryption keys, alarms, control messages and software upgrades. All of this information could potentially be leaked by the meter if proper security mechanisms are not ensured (T15). Messages forwarded through a meter in the mesh network can also be leaked (T17), and information about third-party equipment connected to the meter can be leaked (T18). Communication between meter and HES, and meters in the NAN, can be eavesdropped (T14 and T16 in Table 2.4). Also, communication from a local communication interface can be eavesdropped (T19).

The primary approach to avoid information disclosure is to implement encryption of all communication and ensure preventive measures to meters being compromised.

Denial of service: The goal of Denial of Service (DoS) attacks is to prevent other legitimate users from accessing or using a service. A potential DoS attacks could be to prevent communication between meters to the HES. Unavailable meter data is not considered critical because there exist alternative ways of reporting this data. However, commands or alarms from the HES to the meters could be crucial for various reasons. There are different ways an attacker could perform a DoS attack on the master meter. First of all, he could attack the HES, the meter or communication links (T20-T24 in Table 2.4), which affects I1 and I2. This can be done using, for

example, jamming techniques, or false base stations to redirect and drop traffic. The use of jamming techniques would affect a large number of nodes (T25). Dropping messages could be used on a single node (T26). Secondly, the attacker could perform a Distributed Denial of Service (DDoS) attack where a significant amount of requests are sent from different sources to a meter. This renders the meter unavailable to other legitimate users because it does not have enough resources to process their requests. Malware or other specially crafted messages could also be used to make the meter unavailable (T21). DoS may be caused by errors in the meter software or configuration. It is less likely that third-party equipment can threaten the availability of meters (T27) due to the limited communication on I3. There is a risk that local maintenance causes unavailability on interface I4 (T28). People with physical access to the meter may disable communication (T29).

Elevation of privileges: Elevation of privilege attacks exploits programming errors or design flaws as a mean for the attacker to obtain different privileges than he currently has. Elevated privileges can be used to gain access to data, applications or other parts of a network previously unreachable. We can separate between remote and local attacks. On interface I1, two systems could be compromised remotely, the HES and the meter (T30 and T31 in Table 2.4). Meters could also be attacked remotely via I2 or I3. For a successful attack on I3, the attacker would have to attack via third-party equipment. This includes compromising such equipment remotely. Local attacks are also possible if the attacker has physical access to the meter (T32).

The vulnerability of the systems depends on several factors. For remote access threats, it relies on software quality and how well the system is protected in general. This includes patching regime, the presence of malware protection, and detection software and the security mechanisms controlling remote software updates [TJL13]. Local compromise of the meter should be protected against using physical anti-tampering mechanisms. Furthermore, the meter should be able to detect unauthorized changes.

2.4.4 Motivation for attacks

Understanding the motivations for a cyber attack on the smart meter is important because it can help determine what the attacker wants to achieve. This supports the DSO in the process of pinpointing what to protect and how to protect it. To understand what motivates an attacker to exploit vulnerabilities in the AMI, we first need to identify the assets and associated attack goals. An asset is any hardware, software or other information that supports information-related activities and provides value to an organization. Implementing sufficient security in the smart meter is often a question about cost. More security features require a larger budget. A quantitative assessment can be helpful when allocating a security budget. By identifying the

ID	Name	Interface
Spoofing		
T1	Fake HES	I1
T2	Fake meter ID	I1, I2
T3	Fake master meter	I2
T4	Attacker is authenticated as maintenance personnel	I4
Tampering		
T5	Tamper with communication between HES and master meter	I1
T6	Tamper with communication in mesh network	I2
T7	Tampering before forwarding message	I1, I2
T8	Local maintenance alters meter data or software	I4
T9	Meter reports wrong data to local maintenance	I4
T10	Third party equipment alters meter data or software	I3
Repudiation		
T11	Meter denies having received a message	I1, I2
T12	Meter denies sending of message	I1, I2
T13	Maintenance dispute	I4
Information disclosure		
T14	Eavesdrop on communication between master and HES	I1
T15	Meter leaks configuration information	I1, I2
T16	Eavesdrop on communication in the mesh network	I2
T17	Leaking of forwarded messages	I2
T18	Meter leaks information about third party equipment	I3
T19	Eavesdrop on communication from local comm. interface	I3
Denial of service		
T20	Denial of service attack on HES	I1
T21	Meter errors/attacks make meter unable to communicate with HES	I1
T22	Communication failure on the link between HES and master meter	I1
T23	Meter refuses to communicate with HES	I1
T24	Denial of service attack on meter	I2
T25	Disrupt communication in mesh network	I2
T26	Node lockout	I2
T27	Meter unavailability caused by third party equipment	I3
T28	Meter unavailability due to local maintenance	I4
T29	Physical disabling of meter communication	I4
Elevation of privileges		
T30	Remote access to HES	I1
T31	Remote access to meter	I1, I2, I3
T32	Local meter compromise	I3, I4

Table 2.4: Threats to AML.

different reasons why someone might target the smart meter, and correlating these with his or her associated financial impacts, we can obtain a better understanding of the security risks in the AMI.

According to The White House, *cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century* [Hou09]. It is therefore in the interest of organizations and the government to understand the motivations of cyber-attackers to prevent attacks. The motivations behind cyber-attacks can vary greatly depending on the intention of the attacker. In many cases, the real purpose and primary objective of an attack can be difficult to understand, even if the attacker claims responsibility [SSR13]. However, to more easily understand common motivations, we can categorize attackers. It should be noted that an attacker may belong to multiple categories [AW11]. For example, politically motivated cyber-attacks may be carried out by groups *who use cyberspace to spread propaganda, attack websites, and steal money to fund their activities or to plan and coordinate physical-world crime* [GSM⁺11]. In general, non-political attacks are financially motivated [And11].

Cyber attackers can be separated into two general categories, "outsiders" and "insiders" [RG91]. Insiders act from within an organization and often have knowledge or privileges not considered standard. Outsiders, on the other hand, try to attack an organization or system from the outside. This means they have less knowledge and no privileges which can be used to enhance the success of their attacks.

There are three categories of insiders: 1) disgruntled employees, who may perform retaliatory attacks or threaten internal systems because of a dispute; 2) thieves, who are financially motivated and may manipulate the system for personal gain; and 3) unintentional attackers, who may inadvertently facilitate outside attacks, but are not the primary attacker [AW11].

Outsiders can be more granular classified based on their organization, motives, and professional level. The base categories are organized attackers, hackers, and amateurs. Each of these categories can be further broken down. We will now have a look at each of them.

1. Organized attackers: Can be divided into organizations of terrorists, hacktivists, nation states, and criminal actors. Terrorists are persons *who uses unlawful violence and intimidation, especially against civilians, in the pursuit of political aims* [Dic18]. Hacktivists try to promote a political agenda or social change. Damage may be involved to achieve their goals, but the motivation is primarily to raise awareness, not encourage change through fear [Per12]. Nation-state attackers operate on behalf of governments, collecting information and perform-

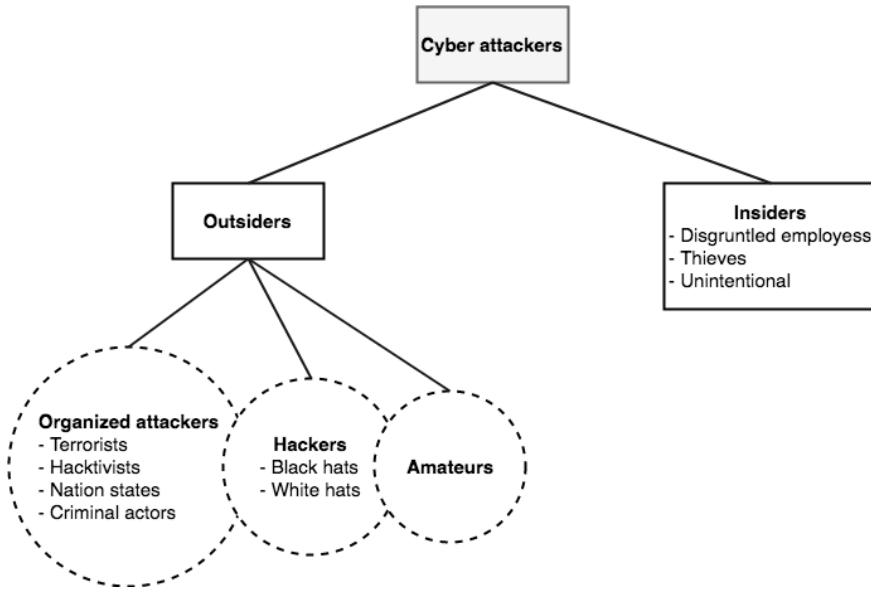


Figure 2.15: Categories of cyber attack [Per12].

ing sabotage. They are often highly trained, well funded, tightly organized, and backed by solid scientific capabilities. Combined with their highly sophisticated attacks directed toward specific goals, it makes them extremely powerful. Nation-state attackers can be hard to categorize since they may be directly employed by an arm of a national government, or they may be an organized crime entity employed by a national government. Professional criminals are usually organized groups [CPS⁺98]. They may operate within complex criminal ecosystems, and are usually financially motivated, albeit control and power are driving factors as well.

2. **Hackers:** Someone who exploit vulnerabilities in a computer system or network to gain information or access through an escalation of privileges. Hackers are often referred to as a single person. Hacking in itself is not a malicious activity, but it is the intention which makes it malicious. "White hat" hackers are people who hack systems to help uncover vulnerabilities, and a contract legally binds their activities and extent of work. "Black hat" hackers, on the other hand, have no agreement with the owner of the system, and the goal is to exploit a system through illegal activities maliciously. Black hat hackers could be hired by criminal organizations or governments with financial or political motivation.
3. **Amateurs:** Less-skilled hackers that most often use existing tools and instructions found on the Internet. Whereas other groups are often financially

motivated, the motivation among amateurs vary. Some may perform cyber attacks out of curiosity or because they seek new challenges. Other may perform cyber attacks as a way to demonstrate their skills and seek admission into a hacker group [AW11]. Although amateurs lack the resources and skills of organized attackers and hackers, they may inflict serious damage if the victim's system is unprotected.

There can be overlap between the different categories. For example, a group of hackers who coordinate cyber attacks could be considered organized attackers. Furthermore, where do we draw the line between an amateur and a professional hacker?

Figure 2.15 illustrates the different categories of cyber attackers. The goal of creating these categories is to understand better the attackers' motivations and the actions they take. There are three types of actions: 1) inadvertent actions, which are often taken by insiders without malicious intent; 2) deliberate actions, performed by insiders and outsiders, and are meant to harm, and 3) inaction, generally by insiders, caused by the lack of action in a given situation. Inaction can be a result of a lack of knowledge, appropriate skills, guidance, or the availability of the correct person to take action [RGSFCMSG18]. Deliberate actions are considered for this thesis since it can be tested. It can be divided into three categories of motivation, which are listed below [Per12]:

- **Political motivations:** Examples include empowerment through destruction, disruption or taking control of targets; espionage; protests, political statements, retaliatory attacks.
- **Economic motivations:** What is maybe considered the primary motivation for cyber attacks. Economic motivation includes theft of intellectual property or other valuable digital assets such as credit card details; fraud; industrial espionage and sabotage; and blackmail.
- **Socio-cultural motivations:** This includes cyber attacks motivated by philosophical, theological, political and even humanitarian goals. *Socio-cultural motivations also include fun, curiosity, and a desire for publicity or ego gratification* [Per12].

The categories of motivation are illustrated in Figure 2.16.

A list of assets and their associated attacks goals are listed in Table 2.5. The assets A2, A3, A4, A6, and A7 are more related to the smart meter and therefore

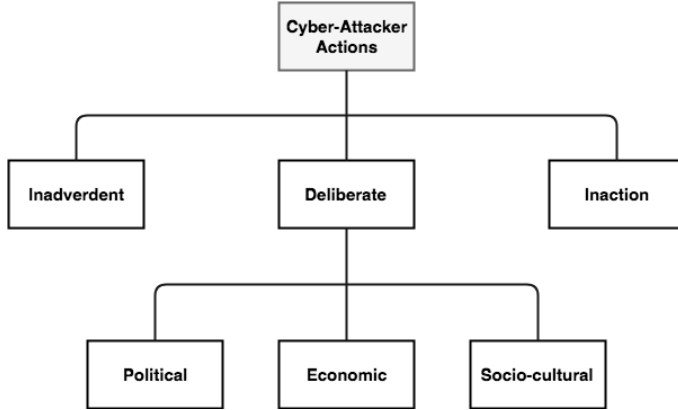


Figure 2.16: Types of cyber-attacker actions and their motivations when deliberate

ID	Asset	Attack goal
A1	The configuration/topology of the power grid	- Get knowledge of the topology of the power grid in order to perform physical or online attacks
A2	The identities of meters (including the ability to authenticate meters)	- Manipulate energy bills by reporting consumption as another meter
A3	Control messages, including messages such as alarms, configuration and software updates and status messages	- Injection of false control messages, in order to manipulate meters (configuration settings, software, keys) - Have meters turn off power
A4	Meter values that can reveal consumption patterns	- Get access to consumption data in order to use this for marketing, or for criminal activities, or other unintended uses - Modify consumption data in order to manipulate bills
A5	The HES	- Break into HES, and the systems beyond HES
A6	The tariffs in meters	- Cause instability of the power grid
A7	The actual meter	- Manipulation of power measurements (stored, reported) in order to reduce bill - Use meter to attack other meters or the HES - Limit the availability to access/control meters

Table 2.5: Assets and associated attack goals.

considered of higher relevance to this thesis. Both insiders and outsiders may attempt to attack these assets, and their motives may be varying. However, we will try to highlight those threats which are more apparent to occur. Note that the motivation for attacks is subjective, and differs between attackers. Manipulation of meter data is a deliberate action with economic motivation. The smart meter discussed in this thesis is first and foremost aimed at private households. It is therefore likely that the type of attacker with economic motivation are amateurs and hackers seeking personal gain. Insiders with good knowledge of the system could also be included since they have inside information on how the system could be exploited. Manipulation of energy bills includes asset A2, A4, and A7. If an attacker can gain unauthorized access to consumption data from consumers, this could be used for criminal activities. For example, the attacker can get insight on when residents in a household are home during the day, and use this information to perform a burglary. It is economically motivated and likely performed by organized criminal actors. Getting access to consumption data includes asset A4. There are also attack goals which are not directly economically motivated. An attacker could manipulate meters and even have them turn off. He could cause instability to the power grid. Furthermore, he could use meters to attack other meters or the HES, or limit the availability to access or control meters. These types of attacks are harder to categorize because it may be unclear what the real intention is. Looking at the scale of the attack is helpful. If the footprint of the attack is significant, then this indicates that the attacker is organized. Amateurs and hackers have limited resources and therefore lack the capabilities of organized attackers. The motivation for attacks that disrupts the power grid are likely political or socio-cultural. Nation states in war would be interested in paralyzing the electric infrastructure of its opponents. Having meters to turn off power is, therefore, a valued attack goal, especially if the attack can be scaled to many meters. Such an attack could be politically motivated and involves asset A3. Terrorists are also possible cyber attackers. With the purpose of inflicting damage to reach political aims, their attack goal can be to cause instability to the power grid or damage it in some other way. Asset A3, A6, and A7 would be attractive targets for terrorists, who are politically motivated.

The financial impact on the DSOs are varying and can be both direct and indirect. Manipulation of meter data creates inaccurate data for billing. This has a direct impact on the revenue for DSOs because they are unable to charge customers for their exact consumption. Any form of attacks that manipulate data may create instability to the grid or otherwise affect the end users. This may have an indirect financial impact because of potential reputational damage to the DSO. However, the DSOs have a monopoly in their operating area, and it is not easy for customers to change DSO. Instability to the grid can also disrupt business operations to DSOs.

2.5 GPRS security for smart meters

The master meter needs to communicate with the HES to provide intended functionality, such as data reporting and receiving commands and updates. In Norway, General Packet Radio Service (GPRS) is primarily used when we talk about 2G. Many smart meter implementations rely on GPRS as a mean of communication [JTK13]. However, GPRS has several shortcomings when it comes to security. These shortcomings essentially affect the security for the smart meter. Before considering security issues in GPRS, we will give a brief introduction to the technology.

2.5.1 GPRS overview

GPRS continues to be used in many places where it is too costly to upgrade the cellular network infrastructure to newer alternatives. It is also a popular choice in many rural settings [Tel13]. GPRS introduces packet oriented mobile data according to the Internet Protocol (IP), which differs from the circuit switched Global System for Mobile communications (GSM). Furthermore, GPRS facilitates much faster data transfer service, typically reaching speeds of 40Kbps [3GP18]. One of the goals of GPRS has been to support bursty traffic and occasional transmission of large amounts of data in an economical way [Huo07]. GPRS attempts to reuse the same components used in GSM and therefore shares the radio network with GSM. However, GPRS introduces some new components to accommodate packet-based communication and therefore has a different core network. A short description of the main components in GPRS is given below.

Mobile Station (MS): Device that can be connected to GPRS services. In the case of AMI, it is the master meter.

Base Transceiver Station (BTS): Responsible for transmitting and receiving radio signals. It also has equipment for encrypting and decrypting communications with the Base Station Controller (BSC).

Serving GPRS Support Node (SGSN): The SGSN serves the smart meters. SGSN primarily handles MS registration and authentication to the GPRS network. It also keeps track of the location of connected devices (MS mobility), performs security functions, and is responsible for sending and receiving data to and from the smart meters.

Gateway GPRS Support Node (GGSN): The GGSN is responsible for interconnecting traffic between the GPRS core network and external packet switched networks, such as the Internet or an X.25 network.

Mobile Switching Center (MSC): The MSC is mostly associated with communications switching functions, such as call set-up, release, and routing.

Home Location Register (HLR): The HLR is a central database which function is to store MS profiles. These profiles holds details of each mobile phone subscriber that is authorized to use the core network. It also contains information about allowed Packet Data Protocol (PDP) per MS as well as allowed PDP addresses per protocol. The PDP is the protocol used to send packets on the network. It can be IP for example [Huo07]. In general there is one central HLR per mobile network operator.

Visitor Location Register (VLR): The VLR is a database that contains information about a subscriber roaming within the location area of a MSC. Its function is to reduce the number of queries that the MSC have to do to the HLR to get information about a subscriber.

Authentication center (AuC): The AuC stores information used to authenticate users of the network. Its functionality is to prevent unauthorized users on the network. Often, the AuC is integrated in the HLR.

Equipment Identity Register (EIR): The EIR contains a list of reported stolen Mobile Equipments (MEs), which the SGSN can use to check the status of a mobile's International Mobile Equipment Identity (IMEI).

These are just some of the components in GPRS, many of which are found in other cellular technologies, e.g., GSM. Figure 2.17 gives an overview of the GPRS core infrastructure with a private Access Point Name (APN). The figure illustrates some of the main components in GPRS but is not complete.

The master meter connects to the BTS which provides the best signal strength. The BTS connects to the SGSN which is one of the main components of the network. Data to and from the SGSN is encapsulated using GPRS Tunneling Protocol (GTP). GTP is designed for tunneling and encapsulation of data units and control messages in GPRS. The GGSN connects the GPRS core network to the Internet, to establish communication with the HES.

2.5.2 Security in GPRS

We will look what the security functionality in GPRS, and some of its shortcomings.

Authentication and key agreement

User authentication procedures in GPRS are similar to the procedures in GSM. The distinction is on what component performs the authentication. In GPRS it is the

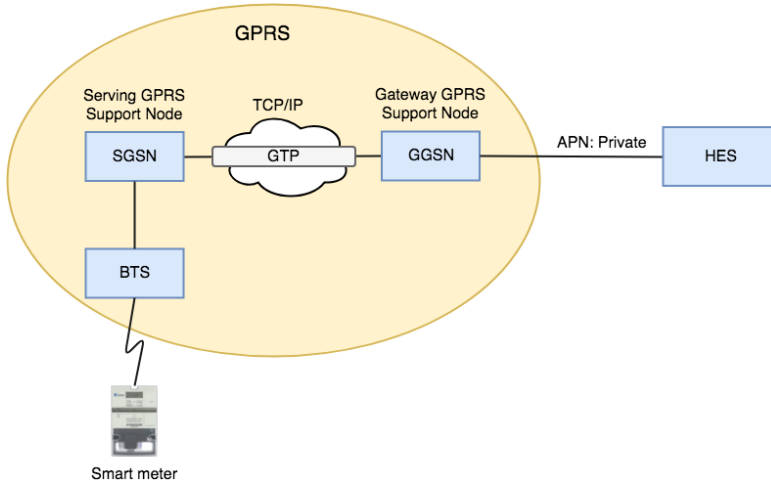


Figure 2.17: Overview of a possible GPRS architecture.

SGSN while in GSM it is the MSC. For further discussions about the protocol, we will, therefore, use the name SGSN. Authentication of the subscriber is done by checking that the subscriber has access to the secret key K_i . The protocol used for authentication in GPRS and GSM is the same, called Authentication and key agreement (AKA) protocol, or GSM-AKA in short. The protocol also performs the selection of the ciphering algorithm and the synchronization for the ciphering. The actual implementation of the protocol is operator dependent. However, the GSM Association supports the operators by giving several example algorithms.

When a MS connects to a GPRS network there are several processes involved, including an attach process, authentication process, and PDP activation process. A pre-requisite for authentication is that the MS has performed the attach process. We will now look at the steps involved in the authentication process which is displayed in Figure 2.18.

1. The VLR/SGSN sends a request for authentication triplet to the HLR/AuC. The International mobile subscriber identity (IMSI) is provided in the request.
2. HLR/AuC produces the triplet and sends it back to the VLR/SGSN.
3. VLR/SGSN sends the challenge (RAND) to the MS.
4. MS replies with a signed response (SRES).

Three cryptographic functions during are used during the authentication process: A3, A5, and A8. A3 for authentication, A5 to encrypt data, and A8 for generating

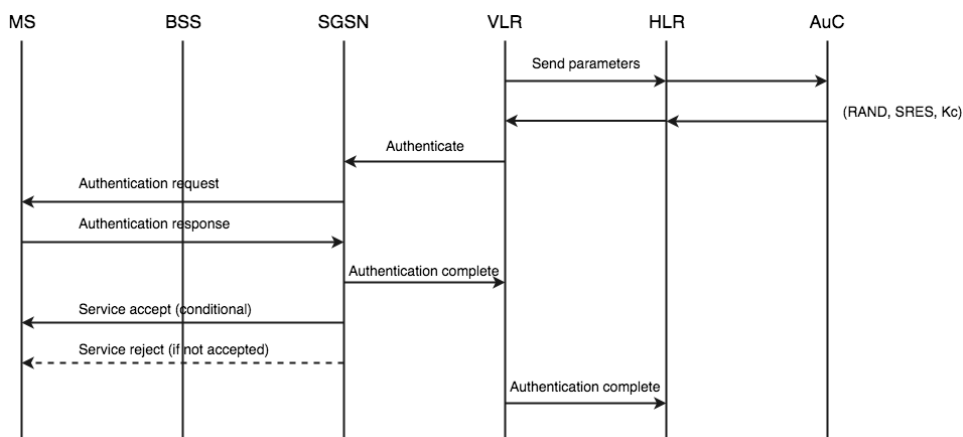


Figure 2.18: Authentication procedure for GPRS. The Base Station Subsystem includes the BST and BSC.

the cipher key K_c . An illustration of the cryptographic functionality is given in Figure 2.19. SIM cards and the AuC uses the authentication function A3 and key generating function A8. To generate the random challenge, the AuC uses a Pseudo Random Number Generator (PRNG). The authentication process is modular in the sense that any algorithms can be used for the functions in the authentication process, as long as the algorithms share the same input and output structure. This modularity means that A3, A5, and A8 refers to families of algorithms rather than to individual algorithms. A3, A8, and the PRNG can all be network operator specific. It is up to the network operator what algorithms to use when implementing the functions since the operator controls both the SIM and the AuC. An operator could, therefore, run proprietary algorithms for these three functions. However, the stream cipher A5 (Linear-feedback shift register (LFST)-based) must be common for all operators with roaming agreement. Otherwise, it would not be possible to encrypt and decrypt data between different operators. Some of the alternative solutions to A5 are A5/0 (Null), A5/1 (CEPT), A5/2 (Export) and A5/3 (Kasumi). There is also an A5/4 variant that uses a 128-bits key. However, this algorithm is hard to introduce because changing the key length affects all the interfaces in the system that carry these keys. It also affects several other network components, such as storage of keys and interoperability between operators that use different key length.

There are several entities involved in the authentication process. The elements used in the protocol are listed in Table 2.6 First, the VLR sends the identity (IMSI) of the authenticating MS to the HLR. The HLR checks the IMSI, and requests an authentication triplet from the AuC. The IMSI of the MS is provided in the request.

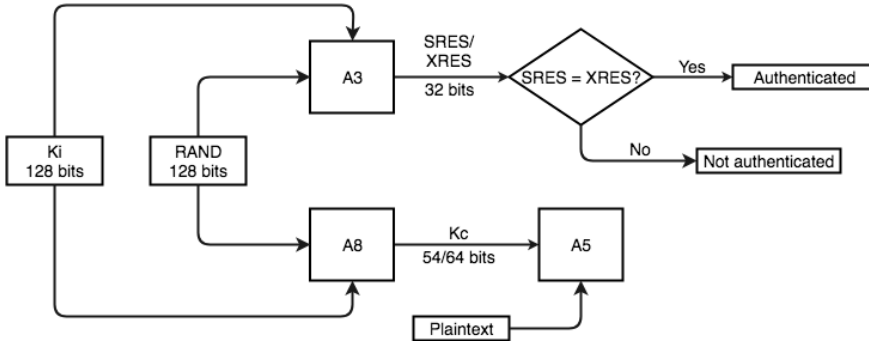


Figure 2.19: Cryptographic functionality used in GSM and GPRS.

K_c	Cipher key calculated by SIM and AuC
K_i	Private key which is shared between SIM and AuC
RAND	Random number between 0 and $2^{128} - 1$ which is used as a random challenge. It is selected by the AuC
SRES	Result of challenge calculated by SIM and sent to SGSN
XRES	Expected result of challenge calculated by AuC, sent to

Table 2.6: Elements used in the GSM-AKA protocol.

The AuC stores the private key K_i and algorithm ID which decides what algorithm is used to produce the session key K_c , and the response to the random challenge (SRES). AuC sends the authentication triplet (RAND, SRES, K_c) back to the HLR which relays it to the VLR. The VLR receives the triplet, stores it, and sends it to the SGSN. Then, an authentication request is sent to the MS from the SGSN, which includes the RAND. The MS produce an authentication response (SRES) to the random challenge using the private key K_i , and sends the response back to the SGSN. The network checks if SRES and XRES are identical. If they are then the MS is authenticated. The SGSN notifies the VLR if authentication is complete, followed by a service accept message to the MS. After that, the VLR sends an authentication complete message to the HLR. A service reject message is sent to the MS if the authentication is not successful.

2.5.3 Assessment of GPRS Security

There are several limitations to the security in GPRS. First of all, the key space for the ciphering key K_c is too small (64 bit). The key space is not considered adequate as the computational power of machines is increasing, making exhaustive key search attacks more effective. The encryption algorithm A5/1 has proven to be

vulnerable against time-memory trade-off attacks [BBK03] [BSW00]. P. Ekdahl and T. Johansson introduced a statistical attack on A5/1 in 2002, enabling a modern PC to carry out a successful attack in less than 5 minutes using limited precomputation time and memory [EJ03]. Active attacks are not addressed by GPRS since it relies on security functionality from GSM. A false base station, often referred to as an IMSI-catcher, can be used to perform a MITM attack between the MS and BTS. The IMSI-catcher masquerades as a base station and lures nearby subscribers to connect by emitting a strong signal. The subscriber will perform the attach procedure to the IMSI-catcher, during which time the attacker obtains their IMSI. The attack is possible because the GSM specification does not include mutual authentication between the MS and the network. The network authenticates the MS using the IMSI. However, the MS does not authenticate the network. It is very hard for the MS to detect the IMSI-catcher. Since the network decides what ciphering algorithm to use for A5, the attacker can exploit this by disabling encrypted traffic (A5/0 flag) or use an algorithm which is broken (A5/1 and A5/2).

It is recommended to use the GSM-Milenage implementation as an alternative to GSM-AKA [JTK13]. It uses the UMTS Milenage AKA functions and a set of conversion functions to implement the A3/A8 functions [JTK13].

UMTS Authentication and Key Agreement

The UMTS Authentication and Key Agreement (UMTS-AKA) protocol can be utilized on top of the GSM Edge Radio Access Network (GERAN) if the subscriber uses a Universal integrated circuit card (UICC) containing the Universal Subscriber Identity Module (USIM) application. The UMTS-AKA protocol is defined in 3GPP TS 33.102 [3GP17b]. We will not go into the full details of this protocol, but highlight some of the main functionality. The UMTS-AKA protocol uses five functions: f_1 , f_2 , f_3 , f_4 , and f_5 . For authentication, function f_1 and f_2 are used. The remaining functions f_3 , f_4 , and f_5 are used as key generating functions. All the five functions take the secret key K_i and random challenge RAND as input. f_1 and f_2 also take a sequence number SQN and an Authentication Management Field (AMF) as input. Figure 2.20 gives an overview of how and where the functions are used. The AuC and each USIM share these functions, as well as the secret key K_i . Furthermore, the AuC contains a random number generator and a sequence number generator, and the USIM contains an algorithm to verify the freshness of received sequence numbers. The resulting outputs from the functions are listed below.

- **MAC:** Message Authentication Code.
- **XRES:** Expected challenge result.
- **CK:** Cipher Key for subsequent message encryption.

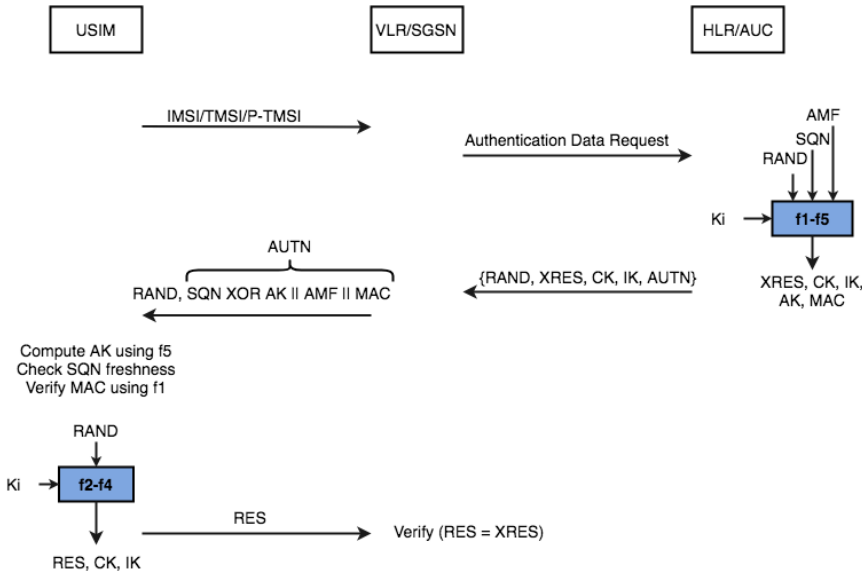


Figure 2.20: UMTS-AKA protocol [Mar16].

- **IK:** Integrity Key.
- **AK:** Anonymity Key (for obfuscating the sequence number in case this exposes the identity of the client).

The AUTN triplet sent from the VLR/SGSN to the USIM is roughly equivalent to the GSM triplet. The elements used during the UMTS-AKA protocol are explained in Table 2.7.

As with GSM and GPRS, the cryptographic functions used in UMTS during the AKA protocol are not standardized, thereby operator dependent. 3GPP has therefore created an informative example algorithm for the f1-f5 functions, called MILENAGE [3GP17a]. MILENAGE relies on a strong 128-bit encryption algorithm as a kernel function, where both block size and key size are 128 bits. AES is recommended for this purpose [Mar16].

UMTS Security Design Plan The design of UMTS set out to correct security weaknesses in GSM and GPRS. Some of the properties that UMTS-AKA introduced are:

- Mutual authentication between the MS and network.

Acronym	Explanation
AK	Anonymity key (48 bit). Produced by: $f_{5K}(\text{RAND})$
AMF	Authentication management field (16 bit)
AUTN	Authentication token (128 bit). Consists of: SQN XOR AK AMF MAC
AV	Authentication vector computed by AuC. Consists of: (RAND, XRES, CK, IK; AUTN)
CK	Cipher key (128 bit). Computed by $f_{3K}(\text{RAND})$
IK	Integrity key (128 bit). Computed by $f_{4K}(\text{RAND})$
K_i	Subscriber authentication key (128 bit)
MAC	Message Authentication Code (64 bit). Computed by: $f_{1K}(\text{SQN} \text{RAND} \text{AMF})$
RAND	Subscriber authentication challenge (128 bit)
RES	32-128 bit result of challenge calculated by USIM and sent to SGSN (default is 64 bit)
SQN	Sequence number (64 bit)
XRES	32-128 bit expected result of challenge calculated by AuC (default is 64 bit)

Table 2.7: Elements used in the UMTS-AKA protocol.

- Fresh session keys derived by using a RAND. The RAND is guaranteed to be fresh because it is protected by the use of the sequence number SQN.
- Integrity protection which is provided by the message authentication code (MAC).
- Longer cipher key for encrypting data. Makes it more resistant to exhaustive brute force attack.
- The MS and network negotiate and agree on what algorithm to use for encryption.
- Confidentiality of the user identity is possible by using a Temporary Mobile Subscriber Identity (TMSI) and AK.
- Generation of new session keys provides forward security.

GPRS encryption

As discussed earlier, GPRS moved the termination point of encryption into the core network at the SGSN. This implied that the encryption function is applied at a higher

communication layer in GPRS. In GSM it was applied at the physical layer, but in GPRS it is applied at the Logical Link Control (LLC). The family of encryption algorithms used in GPRS is called GPRS Encryption Algorithm (GEA), which includes algorithms GEA, GEA2, GEA3, GEA4. The structure of the encryption algorithms is very similar to A5 in GSM. Both the A5 and GEA family are based on a 64-bit K_c , with the exception of A5/4 and GEA4 which uses a 128-bit key. The GEA algorithm is modified to only use 54 significant bits. GEA2 uses 64 bits. GEA3 is based on a Keystream Generator Core (KG-CORE) block cipher mode of operation, which uses the KASUMI block cipher. The KG-CORE primitive is based on a 128-bit key internally [JTK13]. For this to work, the K_c is used twice. GEA4 encryption algorithm also uses a KG-CORE. Since it uses a 128-bit encryption key, it can be used directly as opposed to GEA3. It should be noted that GEA4 requires the subscriber to use a UICC/USIM and run the UMTS-AKA protocol [JTK13].

The encryption algorithm used for communication between the MS and SGSN is determined by the SGSN after the MS has exchanged which version(s) of GEA it supports. If they do not support a common algorithm, then the connection may be released. The SGSN can also decide on not encrypting the data.

GPRS does not provide any built-in security functions that offer confidentiality or integrity protection beyond the SGSN. Data sent from the GGSN to the public internet interface is sent in plaintext. Data between the SGSN and GGSN is sent using GTP, but the protocol does not provide any security.

Security for smart meters using GPRS

The authentication of master meters to the communication network depends on what protocol is used. There are mainly two protocols used, GSM-AKA and UMTS-AKA. Both of the protocols are operator specific, meaning the security relies on what algorithms the operator chooses to use. For GSM-AKA, it is recommended to use the GSM-MILENAGE implementation of A3 and A8 which uses the UMTS Milenage AKA functions. Equipping the smart meter with a UICC/USIM would allow using UMTS-AKA for authentication, and provide increased security over the use of SIM.

The lack of mutual authentication in GSM is a severe vulnerability. As discussed, it allows an attacker to deploy an IMSI-catcher and perform a MITM attack between the MS and the serving network. The equipment used for an IMSI-catcher is inexpensive and requires the user to have a Software Defined Radio (SDR). A SDR is available for as little as 8 dollars on eBay [Kel17]. There is a video on YouTube which demonstrates how to make a cheap IMSI-catcher [Kel17]. The threat of IMSI-catchers can be mitigated by implementing the master meter with a UICC/USIM and performing two-way authentication with the network.

Encryption between the MS and SGSN depends on the algorithms used. With a traditional SIM card, only 64-bit encryption using GEA, GEA2 and GEA3 is supported. However, GEA4 can be used if the smart meter has a USIM installed. Since the smart meter is stationary, it is unlikely that it needs conventional roaming capability. Thus, it could only support GEA4 and advertise this during authentication. The support of this algorithm can be checked beforehand when selecting an operator. It is possible for the SGSN to specify that traffic shall not be encrypted.

2.6 UMTS security for smart meters

In the previous section we talked about the vulnerabilities in GPRS and how an attacker can exploit these. The introduction of 3G was meant to remedy the shortcomings of GSM and GPRS. Universal Mobile Telecommunications System (UMTS) is the mobile technology for 3G used in Norway and most European countries. The security design plan of UMTS was to ensure interoperation and handover with GSM, but correct its vulnerabilities. The standard has been considered secure against MITM attacks since it requires mutual authentication between the mobile station and the network. However, Ulrike Meyer and Susanne Wetzel published a paper on how to perform an active attack on UMTS using the GSM compatibility [MW04]. *The attack allows an intruder to impersonate a valid GSM base station to a UMTS subscriber regardless of the fact that UMTS authentication and key agreement are used* [MW04]. The attacker can use this to eavesdrop on all mobile-station-initiated traffic. The attack is possible because GSM base stations do not support integrity protection. The network authentication in UMTS relies on the validity of the authentication token and the integrity protection of the subsequent security mode command. Thus, mobile stations that support the UTRAN and GSM air interface simultaneously are possible victims. The smart meter provided by Aidon supports both 2G and 3G and should, therefore, in theory, be vulnerable to this type of attack.

2.6.1 UMTS infrastructure

The infrastructure of UMTS is similar to that of GPRS. The MS connects to a base station, called Node B. Base stations are controlled by a Radio Network Controller (RNC). Each RNC can have control over multiple Node Bs. RNCs are controlled by a SGSN or a MSC, depending on if the traffic is packet-switched or circuit-switched. The VLR and SGSN keeps track of the mobile stations which are connected to the Network. Figure 2.21 gives an overview of the UMTS infrastructure. As with GPRS, the IMSI is used to identify subscribers. The IMSI is transported over air interface as infrequent as possible to protect the IMSI. Locally valid Temporary Mobile Subscriber Identities (TMSIs) are also used to identify subscribers and protect the IMSI. UMTS subscribers have a dedicated home network used for identification.

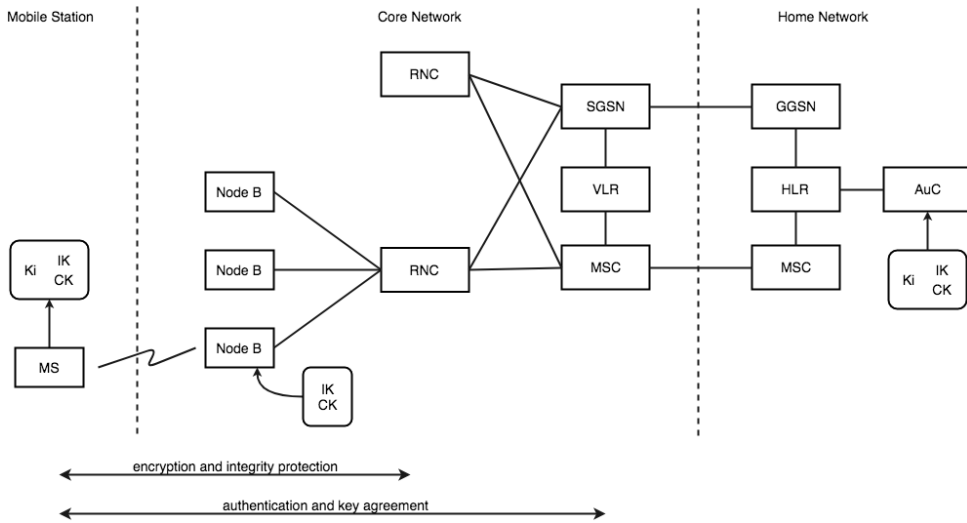


Figure 2.21: Overview of the UMTS infrastructure.

The subscriber shares a long-term secret K_i with the home network. This secret is used for the same purpose as in GPRS, authentication, and encryption.

2.6.2 MITM attack on UMTS

The MITM attack on UMTS is made possible by exploiting the GSM and UMTS interoperability. We will cover some of the basics for the attack. It can be separated into two phases:

- **Phase 1:** The attacker impersonates the victim using its IMSI and obtains a valid authentication token AUTN and RAND by connecting to the real network.
- **Phase 2:** The attacker impersonates a valid GSM base station to the victim's mobile station. The RAND and AUTN from phase 1 are used to fake the serving network. The attacker decides to use no encryption or a broken encryption algorithm. The GSM cipher mode command is sent to the MS which includes the chosen encryption algorithm.

2.6.3 Feasibility of the attack

There are mainly two challenges which the attacker has to overcome to succeed. First, he has to send a valid AUTN token to the victim's mobile station. Secondly,

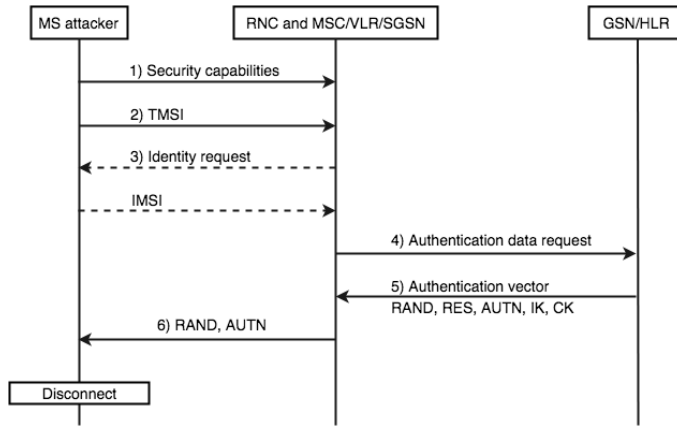


Figure 2.22: Phase 1 - Attacker obtains a valid AUTN and RAND.

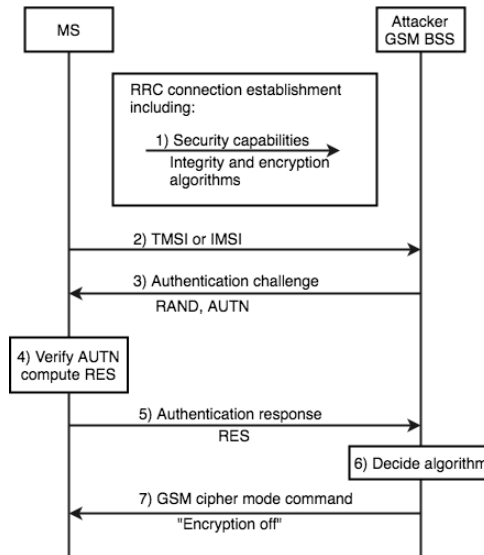


Figure 2.23: Phase 2 - Attacker impersonated a valid GSM base station to the victim and selects no encryption.

he has to ensure that no encryption is used after authentication. The attacker can solve the first challenge by impersonating the victim's mobile station and attempt to connect to the real network. The network will then send him the AUTN. The second challenge is solved by selecting no encryption or using weak encryption in the encryption algorithm command to the MS. The UMTS specification includes an optional setting which allows the user equipment to display the current encryption and integrity protection state. However, this setting is not common to use.

2.6.4 Countermeasures

The MITM attack on UMTS can be avoided by not having GSM and UMTS interworking. Secondly, authenticity check should be added to the cipher mode command message, and security mode capabilities of the mobile station should be included.

Chapter 3

Analysis

The goal of this chapter is to uncover potential vulnerabilities in a smart meter by analyzing its technical specifications and internal components. The results will be used to conduct a risk analysis to help us prioritize what vulnerabilities to further explore during the practical testing. All technical information about the smart meter and Advanced Metering Infrastructure (AMI) has been acquired from Aidon through email and phone correspondence with Rolf Pedersen, Business Development Manager in Aidon, and is considered confidential.

3.1 Security solution for communication interfaces

3.1.1 Communication chain

Aidon aims at providing one or more layers of security for all communication. Such a solution includes end-to-end security for data sent between slave meters or master meters, all the way to the HES. End-to-end security is achieved by using application layer security. Furthermore, Aidon relies on security implemented in the infrastructure used for communication. Figure 3.1 illustrates the security in the communication chain.

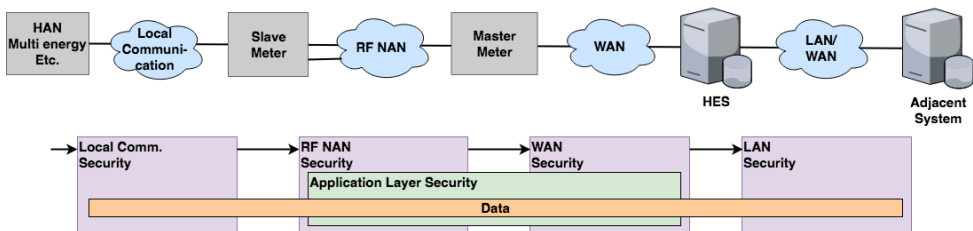


Figure 3.1: Encryption in the communication chain for Aidon AMI.

Local communication security

There is no security implemented on the Home Area Network (HAN) interface today. The communication protocol does not have encryption, and the interface is active by default. Aidon claims that security functionality will be installed in the future once Norwegian Electrotechnical Committee (NEK) have prepared a standard for the security implementation. An alternative has been drafted, but a solution has yet to be finalized. In an email correspondence with Rolf Pedersen, the main points of the temporary draft were presented [Ped18]. In this alternative, the HAN interface has to be activated by the customer. Protocol encryption is applied on the HAN interface. Suggested protocols for encrypting data are EN 62056-7-5 and the security solution according to DLMS Security Suite 0, with reference to the EN 62056-series. Symmetric keys are used for this solution and require a key management system for management of the keys. The customer is responsible for adequate physical security of the HAN interface, while the Distribution Network Operator (DSO) shall secure exterior or common cabinets in which the smart meter resides. The cabinet is secured using a lock provided by the DSO or the customer, according to NEK 399 [53].

The format of the data pushed from the HAN interface is given in table 3.1. Note that this format will change in a future software update, according to Aidon [Ped18]. The data format of today's solution uses explicitly sized data types. Below is a description of the data types:

- U8: unsigned byte (8 bits)
- U16: unsigned word (16 bits)
- U32: unsigned 32-bit value
- U64: unsigned 64-bit value

Unsigned means that the value can only represent non-negative integers. All the data types are in little-endian.

EN 62056-7-5 defines local data transmission profiles for the HAN interface. In the documentation of EN 62056-7-5, one can read that the default configuration of the data link layer only allows unidirectional transmission [Eur17]. The unidirectional transmission should prevent an attacker from uploading malicious content to the meter.

End-to-end and RF NAN security

Data is encrypted between the metering device and HES using application layer encryption. Also, the whole RF Payload (which encapsulates the Application layer)

Field	Data type	Description
METERID	U8[16]	Serial number of the meter
A+	U64	Active Energy import, with resolution of Wh
A-	U64	Active Energy export, with resolution of Wh
R+	U64	Reactive Energy import, with resolution of Varh
R-	U64	Reactive Energy export, with resolution of W
P+	U32	Active import power, with resolution of W
P-	U32	Active export power, with resolution of Var
Q+	U32	Reactive import power, with resolution of Var
Q-	U32	Reactive export power, with resolution of Var
Phi1	U16	Angle between voltage and current L1, with resolution of 0.01 deg
Phi2	U16	Angle between voltage and current L2, with resolution of 0.01 deg
Phi3	U16	Angle between voltage and current L3, with resolution of 0.01 deg
P1	U32	Active power L1, with resolution of W
P2	U32	Active power, L1, with resolution of W
P3	U32	Voltage L3, with resolution of W
U1	U16	Voltage L1, with resolution of 0.1V
U2	U16	Voltage L2, with resolution of 0.1V
U3	U16	Voltage L3, with resolution of 0.1V
I1	U16	Current L1, with resolution of 0.1A
I2	U16	Current L2, with resolution of 0.1A
I3	U16	Current L3, with resolution of 0.1A
F	U16	Network frequency, with resolution of 0.01Hz
PHASES	U8	Type of the meter 1 = single phase meter 2 = three wire meter (phases 1 and 3) 3 = four wire meter (phases 1, 2 and 3)

Table 3.1: The table describes an example of a binary data packet that is sent with a fixed interval from the HAN interface.

is encrypted for messages on the RF NAN (see Figure 3.2). RF encryption is between master and the slave devices. The same encryption algorithm is used to encrypt data on the application layer for communication on the RF NAN and WAN. The algorithm used is based on AES-128 with the Cipher Block Chaining (CBC) mode of operation and a 128-bit key. For the application layer, the integrity check is performed using HMAC-SHA1 and CRC16-CCITT, depending on the message. For the RF Payload, the integrity check is only performed using CRC16-CCITT. CRC16-CCITT uses MAC-then-encrypt (MtE) method, and the HMAC-SHA1 uses Encrypt-then-MAC (EtM). Aidon uses a key hierarchy for encryption and authentication. Each meter uses unique keys for encryption. RF NAN encryption and end-to-end encryption uses different keys. The Microcontroller Unit (MCU) performs the AES-128 encryption,

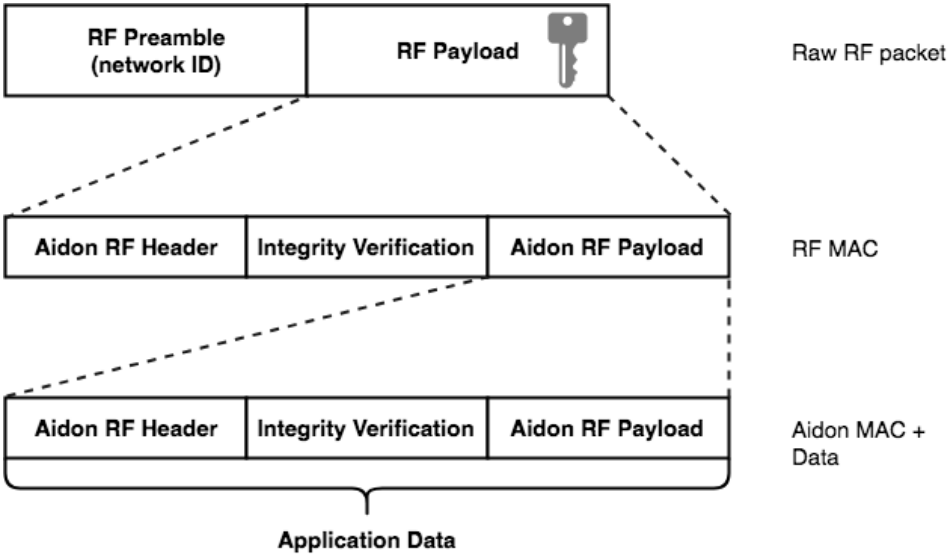


Figure 3.2: Encapsulation of the Application layer in RF NAN.

and stores the encryption keys in its internal flash memory. The MCU flash memory is read protected, and only the firmware can have access to it.

Encryption of data is over the whole RF Payload. As a result, the RF MAC layer messaging (neighbor finding, routing, etc.) is always encrypted, and joining the RF network is possible only if you know the key.

Wide Area Network (WAN) security

All data sent on the WAN is encrypted with end-to-end encryption as previously discussed. Furthermore, master devices are whitelisted in the Head End System (HES). Unknown devices are therefore not able to connect to the HES. The HES performs whitelisting which verifies device identity based on device properties in the message. Firewalls are used on the Mobile Operator and DSO to restrict the allowed connections. The connection between the DSO and mobile operator is made with IPsec VPN. Mobile data is encrypted on the mobile operator level. At last, a private mobile network is used for communication between the master meter and HES. The DSO pays the network company to allocate resources on top of their network infrastructure. Resources on this network are not shared with the public internet, and therefore provides extra security because it is harder for people to intercept the traffic. Only validated UICC cards can communicate to the Access Point Name (APN) of the private network.

3.2 Key management

Aidon handles key management through two components: Aidon Factory System (during device customization) and the HES (during operational use).

3.2.1 Aidon Factory System

Aidon Factory System (AFS) is responsible for creating keys for encryption during the phases of production for the smart meter. We will not discuss the different phases. The keys are stored in the Aidon production keystore, which contains all encryption keys in an encrypted database.

3.2.2 Head-End System

The HES provides key management support during the lifetime of an AMI installation. It supports the main key management processes from an operational point of view, which are:

- Key issuing (create new global or unique keys, automatic).
- Key changing (change one or more keys to one or more devices, manual or scheduled).
- Key invalidation (invalidate keys, automatic).
- Key import/export (e.g., import keys from the factory, manual).
- Whitelist management (e.g., import list of devices from the factory, manual).

An administrator user for the HES can set rules and schedules on when key exchanges are done. An internal database called Keystore hosts the cryptographic keys. The keys are stored in an encrypted format using Key Encryption Keys (KEKs).

All security-related events for the communication between the HES and a device, are logged in the HES. The security log includes events occurring in normal operation and abnormal behavior which has been detected.

3.3 Physical device security

Besides having security implemented on the communication chain, Aidon also provides physical device security. There are several security measures installed as means to prevent and limit potential damage from unauthorized physical access. The device is designed to protect confidential information and report unauthorized modifications.

3.3.1 Sealing and tampering

A cover protects the internals of the smart meter. Removal of this cover creates a Tampering event which is sent to the HES for further investigation. In the case of a loss in main power, the meter is still capable of registering a tamper event by using its integrated backup power for an extended period. The screws used to attach the front cover are sealed, which provide a physical indication whether then the unit has been opened. If an attacker can access the internals of the meter without alerting the HES, it will take more time to detect the occurrence. Any power outage caused to the meter is logged and sent to the HES using built-in backup power. If an attacker cuts the power to prevent the tampering alarm from going off, then the HES is notified of the outage. If the attacker breaks into the device, he needs to access the file system and the firmware to compromise information or cause disturbance to other parts of the collection system.

3.4 Security analysis of specifications

This section discusses some of the security choices for the presented security solution.

3.4.1 Local communication security

First off, there is no encryption on data sent from the HAN interface. Furthermore, the interface is activated by default. Anyone with access to data from the interface can read it in cleartext. There are essentially three ways to access the data: 1) the attacker needs physical access to the HAN interface, 2) the attacker has to read it during transit, or 3) the attacker reads the data from a storage device.

Physical access to the HAN interface depends on how well it is secured. For customers where the meter device resides inside of the household, it is unlikely to be a problem. The attacker would have to break into the household to gain access. For households that are part of an apartment complex, the case may be different. It is common to have meter devices for apartments in an affiliated cabinet, placed in the hallway for example. If the cabinet is not adequately secured, then the HAN interface for multiple meter devices is exposed. An attack scenario could be that the attacker gains access to an unsecured cabinet, mounts a small computer (e.g., Raspberry Pi) with a wireless transmitter to one or more HAN interfaces, and sniffs consumption data from a meter device.

The second and third attack method relies on the customer using the HAN interface to extract data. Having connected devices to create a smarter home is gaining momentum. The worldwide revenue of the smart home market was approximately \$24.1 billion in 2016 and is expected to grow to \$53.45 billion by 2022 [Sta18]. This growth indicates that smart home technology will be a major

force in the digital marketplace of the future, pushing the development of new and innovative solutions. It is a natural step to integrate the smart meters to the smart home environment. The integration can be done in different ways, but the most prominent solution is an integration of the HAN interface to the home network. Such a scenario would only require the attacker to compromise the home network to read the data from the HAN interface. Compromising a home network is considered feasible. Smart home devices have made networks more prone to attacks due to the varying degree of security implemented in devices by manufacturers. For example, a group of hackers attempted to steal data from a North American casino through a fish tank that was connected to the internet [Dev17]. The attackers successfully managed to compromise the tank, revealing information about other vulnerabilities which allowed them to move laterally in the casino's network. A similar approach could be used to attack the home network, and access data in transit or data at rest on some device.

3.4.2 End-to-end and RF NAN security

Data is encrypted on application layer between meter devices and the HES. Data confidentiality thereby remains intact if any of the layers below the application layer is compromised. Also, the RF Payload is encrypted which means that all RF MAC layer messaging (neighbor finding, routing, etc.) is encrypted. Joining the RF network is possible only if the client connecting knows the RF Network key. The algorithm used for encryption is based on AES-128 CBC with a key length of 128 bits. They do not specify the exact implementation, but Advanced Encryption Standard (AES) is considered a reliable cipher which is resistant to brute force and has no theoretical weaknesses in the cipher. The only successful attacks against AES leverage weaknesses in the implementation of the algorithm or key management. The quality of encryption used in the smart meter hinges on how Aidon have implemented the encryption algorithm.

HMAC-SHA1 works well for integrity checking. Although SHA-1 is considered broken, it does not affect HMAC where collisions are not important [Sch05]. HMAC-SHA1 uses Encrypt-then-MAC (EtM) which provides integrity of the ciphertext and plaintext. Also, the MAC does not reveal any information about the plaintext assuming that the output of the cipher is random. Any structure from the plaintext will not be carried over to the MAC. There are no apparent weaknesses to CRC16-CCITT, but it is only used to detect random errors. It does not use a private key as input, and can therefore not provide authenticity of the message, or detect modified messages where the hash has been recalculated. It uses MAC-then-encrypt (MtE) by first producing the CRC16 value of the plaintext, and then encrypting. MtE does not provide integrity on the ciphertext since we have to decrypt the message to determine if it was authentic or spoofed. However, it maintains plaintext integrity.

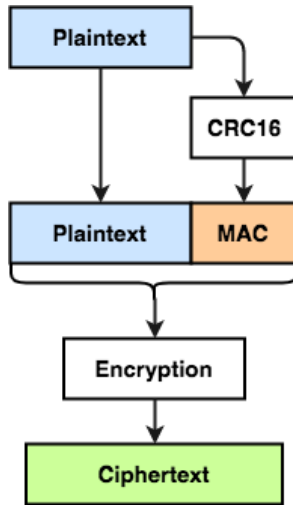


Figure 3.3: MAC-then-encrypt with CRC16.

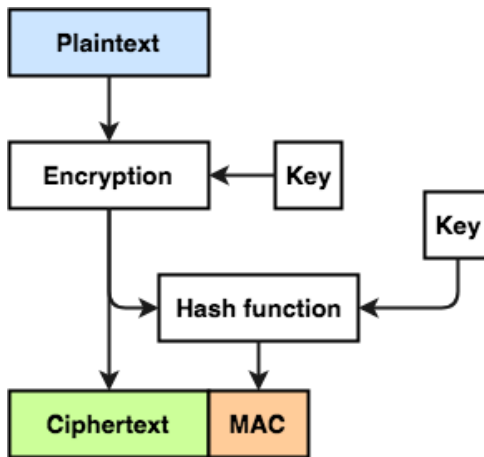


Figure 3.4: Encrypt-then-MAC. Note that different keys should be used as input for the encryption algorithm and hash function.

The Message Authentication Code (MAC) does not provide any information on the plaintext since it has been encrypted. An overview of EtM and MtE is seen in Figure 3.3 and 3.4.

It is unclear why Aidon have chosen to provide integrity checking with both HMAC-SHA1 and CRC16-CCITT. HMAC-SHA1 provides integrity check and authenticity check, while CRC16-CCITT only provides integrity check. It is possible to alter a

message and modify the attached CRC16-CCITT value to be valid because CRC16-CCITT does not take any secret key as input.

Aidon has implemented an extensive key hierarchy for encryption and authentication. It is important that session keys be rotated to provide forward secrecy. Forward secrecy means that the compromise of one session key does not compromise other session keys, or give information that may lead to the compromise of other sessions. Furthermore, it does not give information about the Authentication key (root key). It is difficult for an attacker to obtain the cryptographic keys since they are read protected in the MCU Flash memory.

3.5 Authentication to HES

Authentication over WAN is done using the Remote Authentication Dial-In User Service (RADIUS) protocol [Ped18]. In this section we will discuss how RADIUS works.

3.5.1 RADIUS protocol

RADIUS is commonly used in network environments to control the authentication and authorization for a large number of users with unique authentication information. It provides a centralized user administration, which in this case would be the HES. It is a client/server protocol and runs in the application layer. RADIUS can use either User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) as means of transport. Some of the key features for RADIUS are:

- **Client/server model:** RADIUS operates with a Network Access Server (NAS) which is called the client. This client works as a gateway that controls access to the HES network. The client is responsible for passing information from users to the RADIUS server, and acting on the response it receives back. *The RADIUS server is responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user* [CR00].
- **Network security:** Transactions between the client and server are authenticated through the use of a shared secret. This secret is never transmitted over the network. Passwords sent from the client to the server are encrypted.
- **Flexible Authentication Mechanisms:** The RADIUS server can support various ways of identifying a user. Some of the supported authentication schemes are Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), and Extensible Authentication Protocol (EAP).

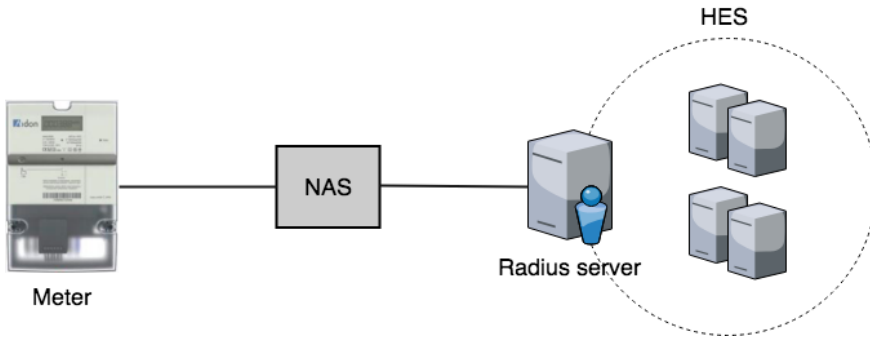


Figure 3.5: Overview of the meter authenticates to the HES using the RADIUS protocol.

- Extensible Protocol: It is possible for vendors of RADIUS hardware and software to implement their own variant of RADIUS using Vendor-Specific Attributes (VSA). It is, therefore, possible that Aidon has developed their own version of RADIUS.

Figure 3.5 gives an overview of how RADIUS authentication is implemented with the AMI.

When a meter attempts to connect to the RADIUS server, it presents some form of access credentials to the client. This may be a username and password, or a security certificate. Once the client receives the information, it can authenticate the user to the server using RADIUS.

The client sends an Access-Request message to the server, containing different attributes of the user. These attributes may be the user’s name, the user’s password, the ID of the client and the Port ID which the user is accessing. If a password is present in the message, it is hidden using a shared secret and the MD5 hashing algorithm. The attributes in the Access-Request are in other words unencrypted, except for User-Password attribute which is protected.

The Access-request is sent to the RADIUS server. Once the RADIUS server receives the Access-Request, it consults a database of users to check if the identity of the request matches any entries. If it does, it also checks if the request meets a list of requirements before granting access. The server can respond in three different ways to the request: Access-Reject, Access-Accept, and Access-Challenge. Figure 3.6 illustrates the possible responses from the RADIUS server. If the request fails to prove the identity of the user, or the user is inactive, then the request is rejected. If the user is identified and meets all requirements, then the server can respond with a

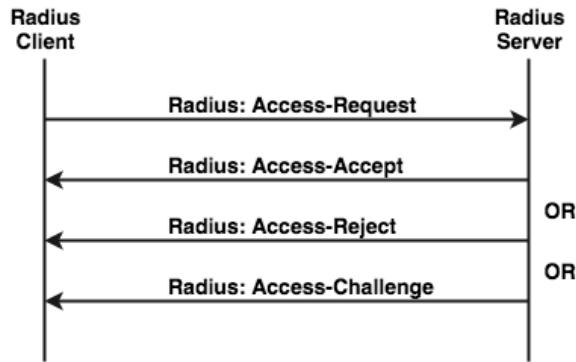


Figure 3.6: RADIUS authentication.

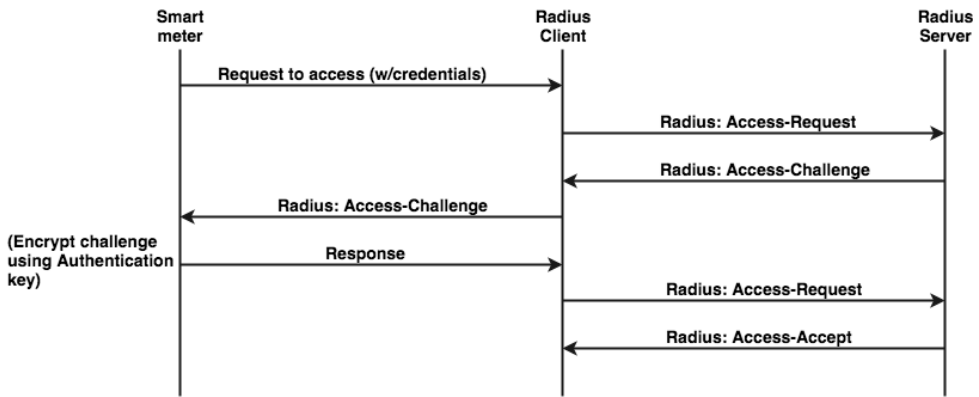


Figure 3.7: Successful RADIUS authentication in Aidon AMI.

challenge. The user receives a random and unpredictable number which it has to encrypt and send back. The response to the challenge is sent in the User-Password attribute. The user sends the answer to the client, which forwards it to the server through an Access-Request message. The challenge-response dialogues are often sent using a secure tunnel. The tunnel is established between the user machine and the RADIUS server such that the access credentials are hidden from the NAS. If the response from the user matches the expected answer, then the server will reply with an Access-Accept message, and give the user access to the network. Otherwise, it will respond with an Access-Reject. A successful RADIUS authentication to the HES may look like something in Figure 3.7.

Interoperation with PAP and CHAP If PAP is used, the NAS takes the PAP ID and password, and sends them in an Access-Request packet as the User-Name

and User-Password. The NAS may include some other attributes as well which we will not cover.

For CHAP, the NAS generates a random challenge (preferably 16 octets) and sends it to the user, who returns a CHAP response along with a CHAP ID and CHAP username. Then, it sends the Access-Request packet to the RADIUS server. The Access-Request contains the CHAP username as the User-Name and the CHAP ID and CHAP response as the CHAP-Password. The random challenge can be included in the CHAP-Challenge attribute or in the Request Authenticator field of the Access-Request packet, depending on how long the challenge is. Once the RADIUS server receives the Access-Request, it looks up the password based on the User-Name. Then, it encrypts the challenge using MD5 on the CHAP ID octet, the password, and the CHAP challenge and compares that result to the CHAP-Password. If they match, the server sends back an Access-Accept. Otherwise, it sends back an Access-Reject.

Use of MD5 in RADIUS

It is likely that Aidon uses the CHAP authentication scheme because they have implemented a key hierarchy which is suitable for the challenge-response authentication. However, they have not confirmed which authentication scheme they use. If the PAP authentication scheme is used, then it may have some consequences because MD5 is considered broken [Ins08]. We will, therefore, include how MD5 is used. Some of the implications will be discussed later in this thesis.

When the client receives a request from a user, it creates the Access-Request packet which is sent to the RADIUS server. A summary of a RADIUS packet is given in Figure 3.8.

For PAP, the credentials of the user attempting to connect are put in the Attributes field. The client generates the Identifier field. The generation of this field is not specified in the RADIUS protocol specification. Normally, a counter is implemented which increments for each request. The Access-Request contains a random 16-byte Request Authenticator in the Authenticator field. As mentioned, the packet is unprotected, except for the User-Password in the Attributes field. The User-Password field is protected as follows:

The NAS and RADIUS server share a secret. That shared secret followed by the Request Authenticator is put through a one-way MD5 hash to create a 16-byte digest value which is XORed with the password entered by the user, and the XORed result placed in the User-Password attribute in the Access-Request packet [CR00].

Upon a request from a client, the RADIUS server verifies if it has the shared

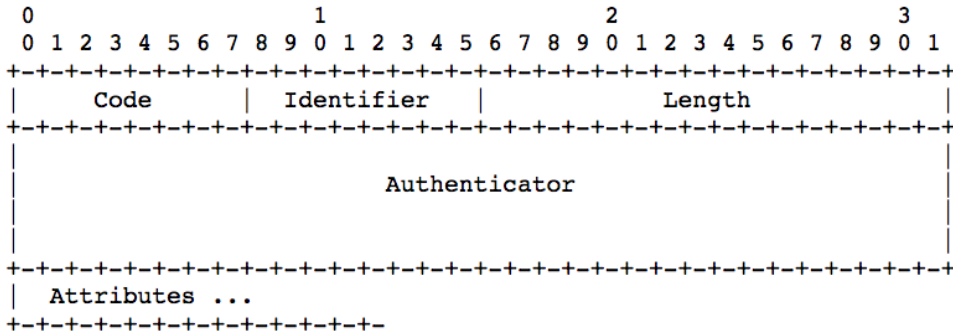


Figure 3.8: A summary of the RADIUS packet [CR00].

secret for the client. When the RADIUS server responds with an Access-Accept packet or an Access-Reject packet, it uses the same Identifier value that it received from the client’s Access-Request packet. A new Response Authenticator is generated for the Authenticator field. The server calculates the Response Authenticator by taking the MD5 hash of the response packet with the associated request packet’s Request Authenticator in the Authenticator field and concatenates it with the shared secret. It looks like this:

$\text{ResponseAuth} = \text{MD5}(\text{Code}|\text{ID}|\text{Length}|\text{RequestAuth}|\text{Attributes}|\text{Secret})$, where $|$ denotes concatenation.

The client does two things when it receives a reply from the server. First, it attempts to match the response with an outstanding request using the identifier field. Then it verifies the Response Authenticator in the received packet. This is done by performing the same Response Authenticator calculation as the server and then comparing the result with the Authenticator field. The client drops the packet if either the identifier field or the Authenticator field does not match.

3.6 Physical inspection of smart meter

A physical inspection of the smart meter and its internals have been conducted to gain information about components used. This information may be valuable for an attacker since it increases the knowledge of the system to attack. Furthermore, it might reveal components with known vulnerabilities. The pictures in this section illustrate the process of disassembling the smart meter.

First, the terminal sealing is detached from the meter device by loosening the



Figure 3.9: The indicated screws are used to attach the terminal sealing on the smart meter.

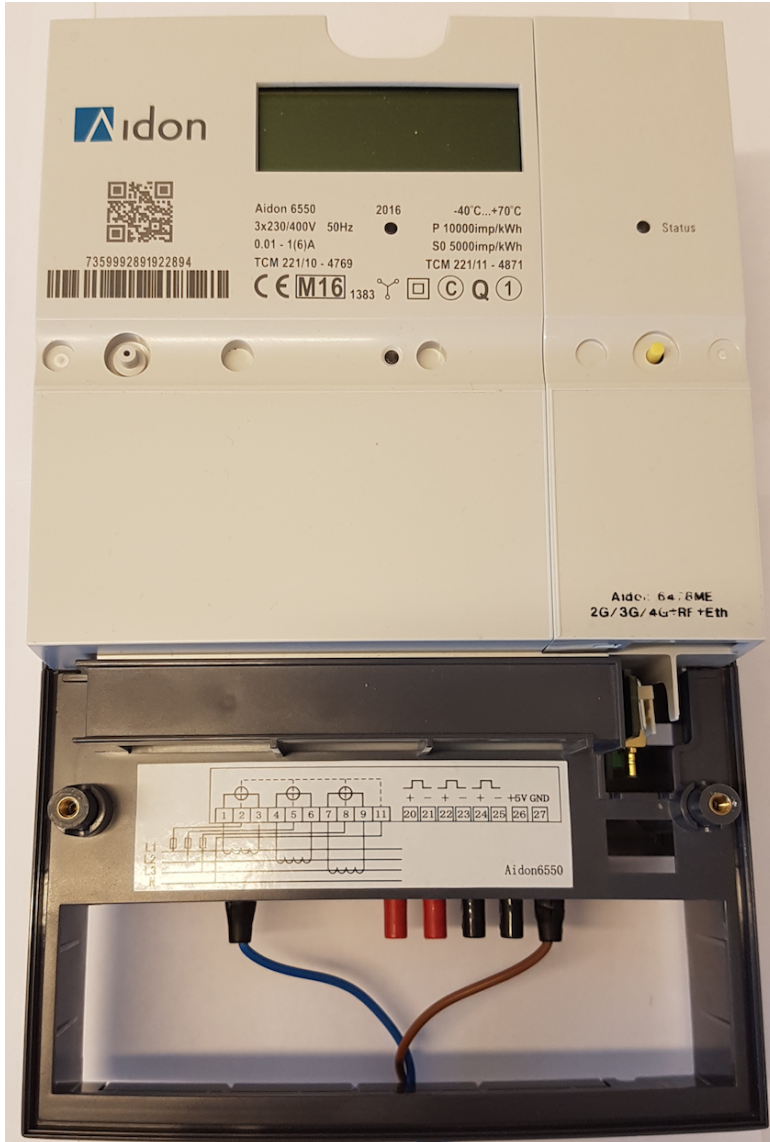


Figure 3.10: Smart meter with the terminal sealing removed.



Figure 3.11: Smart meter with terminal sealing and interface protection removed.

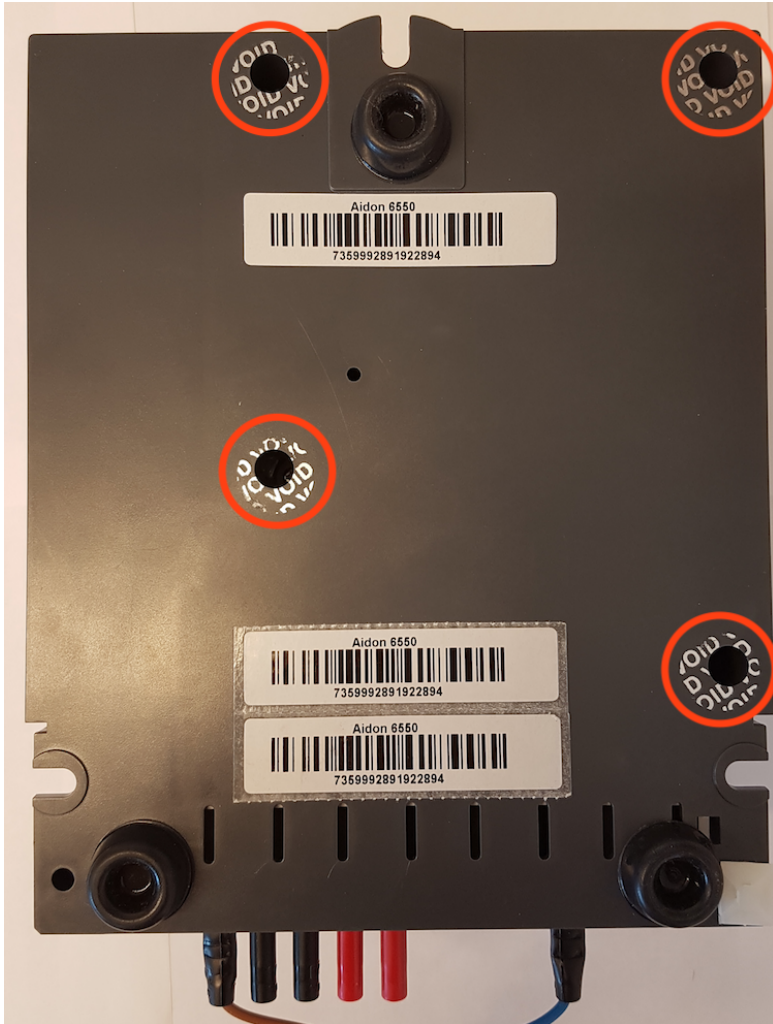


Figure 3.12: The red circles outline the metering unit's screws used to hold the front cover. They are covered in plastic stickers which have been removed in this picture.

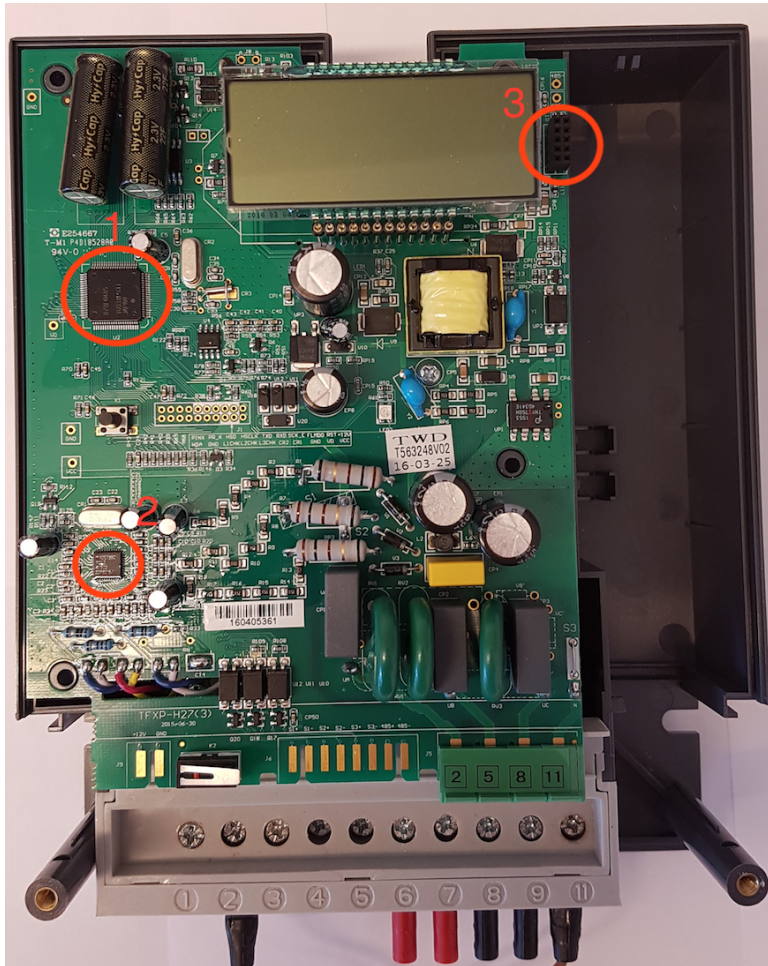


Figure 3.13: The internal components of the meter device. 1) Micro controller unit; 2) Multifunction Energy Metering Integrated Circuit; 3) 10 pin connection for communication module.

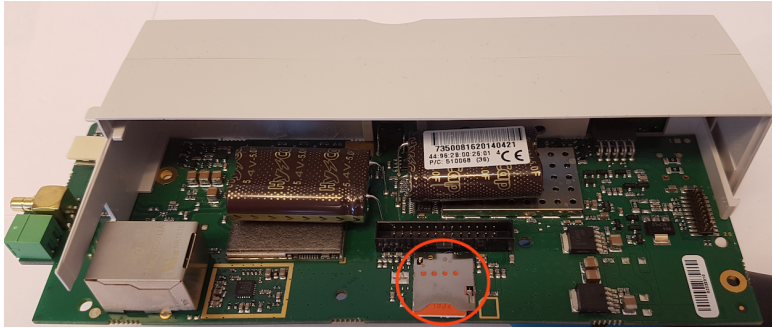


Figure 3.14: Communication module used for the meter device. The red circle outlines the SIM card tray slot.

two screws in Figure 3.9. Removal of the terminal sealing exposes the meter’s main external interface which provides the possibility to attach external modules to the meter (see Figure 3.10). The black plastic frame is easily removable and is used to protect the power connection up front (where the cables leading electricity are attached). Figure 3.11 shows the meter with both the terminal sealing and plastic frame removed. Four screws on the back of the device are removed to detach the front cover and expose the internals of the meter (see Figure 3.12). The screws are sealed. Figure 3.13 shows the internal components of the meter. The meter is modular, and the system module is attached to the main circuit board through a 10-pin interface, outlined in the top right corner of Figure 3.13. The two other components outlined are the MCU and a Multifunction Energy Metering Integrated Circuit (EMIC). The communication module contains a SIM card used for communication over 2G, 3G or 4G (see Figure 3.14).

3.6.1 Components on circuit board

Two of the identified components on the circuit board are highlighted. These are the MCU and EMIC (Figure 3.13), which operate close to the core functionality of the smart meter. Some of their functionality is to measure electricity usage and handle consumption data.

Micro Controller Unit: The MCU installed on the meter is called D78F0485, produced by Renesas Electronics. The user’s manual is accessible on the internet and contains detailed information about the functionality of the MCU [PDF18]. The MCU helps with the registration of energy consumption. Also, the MCU is responsible for data storing, LCD control, external interface handling, keeping track of alarms, events and time, and encryption of data.

Multifunction Energy Metering Integrated Circuit: The ADE7880 is a 3-

phase electrical energy measurement Integrated Circuit (IC). The main functionality of the component is to measure electricity consumption and convert the result to a digital format which is sent to the HES. More information about the ADE7880 is found on the producer’s website [Dev18].

The information in the documentation for the MCU and EMIC could potentially contain useful information. For example, information on how to access the internal flash memory on the MCU. Due to limited time, we will not explore the documentation on the MCU and EMIC any further.

3.7 Risk analysis

When deciding what potential vulnerabilities to test for in the smart meter, there are two factors to take into consideration. These are the risk of the vulnerability, and the feasibility of performing a test for the vulnerability. We want to perform feasible tests of vulnerabilities with high risk. Given these factors, we will select a limited amount of technical risks associated with the smart meter and test these. We will conduct a risk analysis based on the OWASP Risk Rating Methodology [OWA16] to identify vulnerabilities and estimate the associated risk to the business of the DSO. The OWASP methodology is customized for application security. We will modify it to suit the testing of the smart meter, and some of the terms and steps may, therefore, be different. This thesis uses a risk analysis template created for a security report in the course Software Security (TDT4237) at Norwegian University of Science and Technology (NTNU) [TH16].

The approach for the risk analysis is to identify business assets, business risks, and technical risks. The business assets help us identify valuable assets for the DSO which they want to protect. The business risks are non-technical risks that are directly or indirectly related to the business assets. Business risks are associated with one or more technical risks. The business risks and technical risks will be classified using a risk matrix, before commencing the testing. Normally one would also include business goals and objectives in a risk analysis. *Business goals and objectives guide a business toward certain ends. They manifest the intentions of the business and set the course further. Business goals define what the company wants to achieve, while objectives define intermediate milestones toward that outcome* [TH16]. Business goals are excluded from the report since we do not have adequate knowledge of the goals and objectives of the DSOs. It does not have any major effect on the testing. Note that threats to the AMI have already been identified in the threat model in Subsection 2.4.3.

Core business assets	
ID	Description
A.1	Grid infrastructure
A.2	Advanced metering infrastructure
A.3	Consumption data
A.4	Customer information.

Table 3.2: Business assets for grid companies.

3.7.1 Business assets

Business assets are anything that provides value to the company, whether it by tangible objects, intellectual property, or information. There are other definitions, such as *a business asset is a piece of property or equipment purchased exclusively or primarily for business use* [Inv18]. However, we will not use such a rigid definition as cyber security risks more often relate to things in the cyber domain.

The core business assets for DSOs are listed in table 3.2. They are grid infrastructure, advanced metering infrastructure, power consumption data and customer information. The components that constitute the grid infrastructure are essential to provide customers with electricity (A.1). The AMI assures correct meter readings and other features (A.2). Consumption data is used for load balancing and billing (A.3). Customer information is information that DSOs store about each customer (A.4). Customer information may be personal information used for billing, or other analytic data that a DSO may produce about its customers.

3.7.2 Risk matrix

Business risks and technical risks will be graded according to their *probability* and their potential *impact*. Probabilities, as well as impacts, are denoted as (VL) Very low, (L) Low, (M) Medium, (H) High or (VH) Very high. The different *risks* are denoted as (L) Low, (M) Medium or (H) High. The procedure for mapping quantities of probability and impact to a quantity of risk is illustrated in the risk matrix in Figure 3.15.

It is usually not beneficial for a business to implement measures against *all* risks. It is more cost-efficient to prioritize mitigation of risks that constitute the highest impact on the business and to merely neglect risks that may be expensive to mitigate but easy to tolerate. The risk matrix is a beneficial, graphical tool to manage the priorities.

In Figure 3.15, red entries are unacceptable risks that need to be mitigated.

Risk matrix						
Impact	(VH) Very high	(M) Medium	(H) High	(H) High	(H) High	(H) High
	(H) High	(M) Medium	(M) Medium	(H) High	(H) High	(H) High
	(M) Medium	(M) Medium	(M) Medium	(M) Medium	(H) High	(H) High
	(L) Low	(L) Low	(L) Low	(M) Medium	(M) Medium	(H) High
	(VL) Very low	(L) Low	(L) Low	(L) Low	(M) Medium	(M) Medium
	(VL) Very low	(L) Low	(M) Medium	(H) High	(VH) Very high	
Probability						

Figure 3.15: Graphical risk matrix employed in this report.

Yellow entries are medium impact risks that the business needs to evaluate the cost-effectiveness of mitigating. Green entries are acceptable risks that the business could neglect in good conscience.

There are several factors to take into considerations to estimate the impact. These factors are separated into two categories: technical impact factors and business impact factors.

Technical impact factors: Can be broken down into four factors that align with the traditional areas of concern in security. These are confidentiality, integrity, availability, and accountability. The first three factors are known as the CIA-triad. The following description of the four factors are from OWASP [OWA16]:

- **Loss of confidentiality:** How much data could be disclosed and how sensitive is it?

- **Loss of integrity:** How much data could be corrupted and how damaged is it?
- **Loss of availability:** How much service could be lost and how vital is it?
- **Loss of accountability:** Are the threat agents' actions traceable to an individual?

Business impact factors: These factors stem from the technical impact factors but focuses on what is important to the company and its business. To put short, they are what justifies the investment of fixing security problems. Therefore, the factors may be different for companies depending on what business they are operating and their goals. However, OWASP has compiled a list of what they consider common factors [OWA16]:

- **Financial damage:** How much financial damage will result from an exploit?
- **Reputation damage:** Would an exploit result in reputation damage that would harm the business?
- **Non-compliance:** How much exposure does non-compliance introduce? ¹
- **Privacy violation:** How much personally identifiable information could be disclosed?

Note that the evaluation of business risks and technical risks is subjective. We try to depict a realistic and accurate image of the security risk landscape given current knowledge and experience within security, AMI, and smart meters.

3.7.3 Business risks

Usually, the business risks are associated with the strategic direction of a company. This analysis is more general and does not focus on a single DSO. The business risks will, therefore, be a result of what we assume is applicable for most DSO. Table 3.3 summarizes the business risks. B.1 refers to the risk of attacks on the grid infrastructure that may cause power outage of instabilities in the grid. B.2 refers to cyber attacks on the AMI which may disturb operational functions. B.1 and B.2 can cause financial damage to a DSO because they are not able to provide their service (delivering electricity) and properly bill customers. Furthermore, it affects the reputation of the company if customers are unsatisfied with their service. Exposure of customer credentials (B.3) and exposure of consumption data (B.4) are

¹Risk exposure is a measure of possible future loss.

Business risks				
ID	Description	Prob.	Impact	Risk
B.1	Components of grid infrastructure is unavailable	L	VH	H
B.2	Components of AMI is unavailable	M	M	M
B.3	Exposure of customer credentials	VL	H	M
B.4	Exposure of consumption data	L	H	M
B.5	Manipulation of consumption data	L	H	M

Table 3.3: Business Risk Table.

risks that break confidentiality. Data leakage may cause reputational damage. People today are more aware of security and their personal data after the security scandals with companies such as Facebook [CJ18] where user data was leaked. If sensitive data is leaked due to non-compliance with data protection regulations, then this can have financial damage and cause negative exposure. Manipulation of consumption data (B.5) causes incorrect billing of customers and may cause disturbances to the instantaneous balance in the grid. The consequences are a break in the integrity of consumption data and possibly a break in the availability of electrical power.

Figure 3.16 shows a mapping of business risks using the risk matrix in Figure 3.15. One risk item is in the red zone which means that it should be the first risk to mitigate. The other risks are considered of medium impact. Nevertheless, they should be mitigated, but it is not as urgent.

3.7.4 Technical risks

A technical risk can be thought of as a potential technical shortcoming, or vulnerability, that may or may not be exploited by an adversary. Table 3.4 lists the technical risks identified on the communication interfaces on the smart meter. Each technical risk is labeled with a probability and impact.

Figure 3.17 shows a mapping of technical risks to the risk matrix in Figure 3.15. Five technical risks are in the red zone and should be mitigated immediately if present in the system. We consider the remaining technical risk of medium impact. Nevertheless, it is recommended to mitigate those as well.

Consequence	(VH) Very high		B.1			
	(H) High	B.3	B.4 B.5			
	(M) Medium			B.2		
	(L) Low					
	(VL) Very low					
		(VL) Very low	(L) Low	(M) Medium	(H) High	(VH) Very high
Probability						

Figure 3.16: Mapping of identified business risks.

3.7.5 Testing plan

A test plan has been created to determine the presence of the technical risks. The test plan gives an overview of the technical risks and a short test description on how to test for the potential vulnerability. Since there can be conducted several tests for each technical risk, each test case is denoted with a test priority ranging from 1 to 3. 1 indicates low priority, 2 indicates medium priority, and 3 indicates high priority. Tests that are easy to conduct and likely to yield conclusive results are given higher priority.

ID	Description	Prob.	Impact	Risk	Security Requirements	Related business risk	Related threat on AMI
TR.1	HAN interface sends unencrypted data	VH	H	H	Use secure encryption of data from the HAN interface	B.3, B.4	T19
TR.2	HAN interface accepts untrusted data	L	VH	H	Authenticate connection or block all incoming data	B.2, B.3, B.4, B.5	T10, T27, T31, T32
TR.3	RS232 interface sends unencrypted data	H	L	M	Use secure encryption of data from the interface	B.3, B.4	T19
TR.4	RS232 interface accepts untrusted data	L	VH	H	Authenticate connection or block all incoming data	B.2, B.3, B.4, B.5,	T10, T27, T32
TR.5	No mutual authentication between the master meter and HES	L	VH	H	Use secure mutual authentication between master meter and HES	B.2, B.3, B.4, B.5	T1, T2, T5, T7, T11, T12, T14, T15, T20, T21, T22, T23, T30, T31
TR.6	Cryptographic keys not sufficiently protected on meter	L	H	M	Use read protection on memory where keys are stored and ensure authorized access to keys	B.3, B.4, B.5	T3, T14, T16
TR.7	Encryption algorithm is not correctly implemented	VL	H	M	Use well known encryption standards	B.3, B.4, B.5	T3, T14, T16
TR.8	Meter allows execution of arbitrary commands on the host operating system via a vulnerable application	L	VH	H	Authenticate connection or block all incoming data. Implement sufficient input validation	B.2, B.3, B.4, B.5	T10, T27, T32

Table 3.4: Technical risk table.

Consequence	(VH) Very high		TR 2, 4, 5, 8			
	(H) High	TR 7	TR 6			TR 1
	(M) Medium					
	(L) Low				TR 3	
	(VL) Very low					
	(VL) Very low	(L) Low	(M) Medium	(H) High	(VH) Very high	
Probability						

Figure 3.17: Mapping of identified technical risks to the risk matrix in Figure 3.15.

Technical Risk	Test Case ID	Test Priority (1-3)	Test Description
TR.1	C.1	3	Read data from HAN interface using a M-Bus converter and serial port communications program. Inspect data.
TR.2	C.2	3	Upload data to HAN interface using a M-Bus converter and serial port communications program.
TR.3	C.3	2	Read data from interface using a RS232 serial cable and a serial port communications program.
TR.4	C.4	2	Upload data to interface using a RS232 serial cable and a serial port communications program.
TR.5	C.5	3	Configure computer with a local network and DHCP server capabilities. Connect meter to the computer using an ethernet cable. Assign the meter and IP address, and attempt to communicate with it. Capture data from the communication and analyze it in Wireshark.
TR.6	C.6	2	Use JTAG security testing on the meter's circuit board to access the MCU flash memory directly. Attempt to read the data and identify keys.
TR.7	C.7	2	Analyze data sent between the master meter and HES using software and manual analysis. Try to identify flaws in the encryption algorithm implementation.
TR.8	C.8	3	Use Minicom runscript feature to execute UNIX login script and obtain shell access. Launch commands through shell.

Table 3.5: Testing plan.

Chapter 4

Testing

This chapter includes test C.1, C.2, C.3, C.4, C.5, and C.8 from the testing plan. It does not include test C.6 and C.7 because we did not have time to perform the tests. This chapter is structured with a section for each test, named by their test case ID. Some of the tests are grouped because they require similar equipment and setup. Test C.8 is included in two different setups because we attempted to get shell access using both the HAN and RS232 interface. All tests include the equipment used, setup, method, and results. This format creates consistency in the testing and enables others to reproduce the same results.

A desktop computer running Ubuntu 16.04 was used to run necessary software tools for the tests. Note that all terminal commands listed in this chapter are from the Linux terminal. Some of them are bash commands while some are software specific commands.

The attempted file uploads were done with two text files of 16 bytes and 54.5 kB. We created the 16-byte text file ourselves, while the other text file of 54.5 kB was a random text file from our computer.

The conducted tests may produce results that need further exploration. Additional tests may, therefore, be appended to each test case.

4.1 Test C.1, C.2, and C.8

4.1.1 Equipment

- Computer
- Aidon 6550 smart meter with Aidon 6478 system module
- USB to M-Bus slave module

- Minicom 2.7 (or any other serial port communications program)

Four components are used to communicate with the HAN interface. First of is the smart meter itself. For this test, we used the Aidon 6550 smart meter with an Aidon 6478 system module. The HAN interface is compatible with all Aidon 6000 series meter types, and the following system modules provide the HAN interface: Aidon 6476, Aidon 6478, Aidon 6481. A USB to M-Bus slave module reader is required to convert the M-Bus signal into data which the computer can read. A desktop computer running Ubuntu 16.04 operating system is used to run relevant software for the tests. Minicom is used to read data sent from the M-Bus converter, and to send data.

4.1.2 Setup

The M-Bus converter is connected to the HAN interface on the meter device. Figure 4.1 shows the M-Bus converter. The HAN interface has two pins:

- PIN1: GND
- PIN2: +24 M-Bus TXD

For the M-Bus converter used in this test, the blue cable connects to PIN1, and the red cable connects to PIN2. This is illustrated in Figure 4.2 and 4.3. After setting up the hardware, the M-Bus converter is connected to the computer using USB. The converter takes input from the meter device, converts it, and sends the output to the USB interface.

Any serial port reader can be used to read and send data from the USB interface on a computer. In this test, we used Minicom, which is a text-based serial port communications program. To read and send data, Minicom needs to be configured for the correct data channel. Aidon uses the following parameters in the configuration of the data channel:

- Baud rate: 9600 bps
- 8 data bits
- No parity
- One stop bit

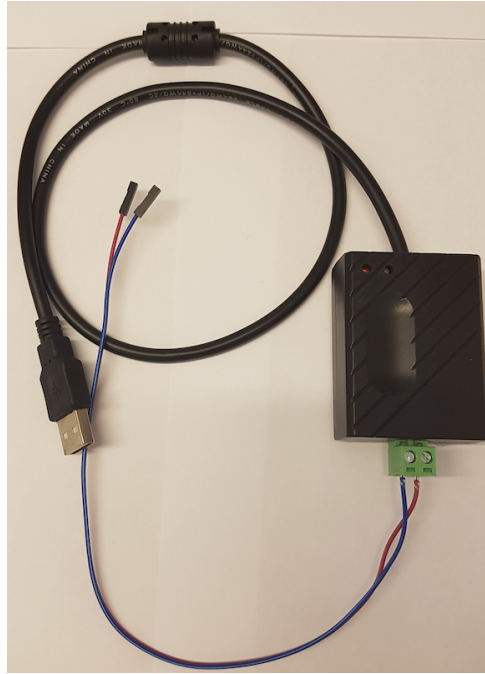


Figure 4.1: M-Bus converter.

The last three parameters are referred to as 8N1.

Furthermore, it must be defined which serial port Minicom should use. Since the M-Bus converter uses USB to connect to the computer, we need to configure Minicom to use the correct USB serial device. To find the name of the port, enter the following in the terminal:

```
dmesg | grep tty
```

This gives us something like this:

```
[ 0.000000] console [tty0] enabled
[ 0.833680] 00:03: ttyS0 at I/O 0x3f8 (irq = 4, base_baud
= 115200) is a 16550A
[ 0.855690] 0000:00:16.3: ttyS4 at I/O 0x3180 (irq = 17,
base_baud = 115200) is a 16550A
[ 238.358591] usb 1-1.3: FTDI USB Serial Device converter
now attached to ttyUSB0
```

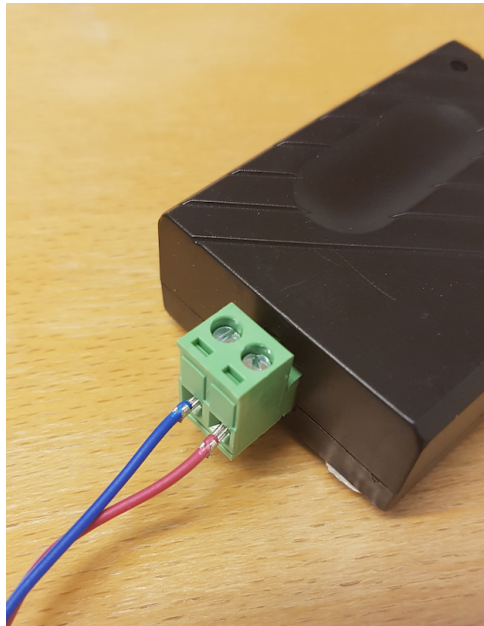


Figure 4.2: The blue cable connects to PIN1 and the red cable connects to PIN2 on the HAN interface.

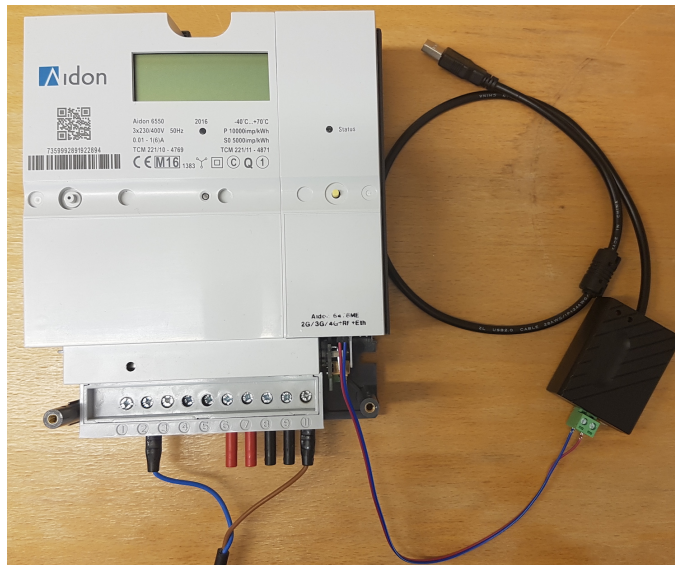


Figure 4.3: Overview of the M-Bus converter connected to the meter device.


```

henrik@ntnu-kontor: ~
Welcome to minicom 2.7

OPTI+-----+
Comp| A -   Serial Device       : /dev/ttyUSB0
Port| B - Lockfile Location     : /home/henrik/Documents/Minicom
    | C -   Callin Program      :
Pres| D - Callout Program       :
    | E -   Bps/Par/Bits       : 9600 8N1
    | F - Hardware Flow Control : No
    | G - Software Flow Control : No
    |
    | Change which setting? █
    +-----+
    | Screen and keyboard   |
    | Save setup as dfl     |
    | Save setup as..      |
    | Exit                  |
    +-----+

CTRL-A Z for help | 9600 8N1 | NOR | Minicom 2.7 | VT102 | Offline | ttyUSB0

```

Figure 4.4: Configuration of the data channel for the HAN interface.

On the last line, we can see that the converter is attached to *ttyUSB0*. *ttyUSB0* is the port we want to use in Minicom. To configure this, enter:

```
sudo minicom -s
```

Next, choose "Serial port setup" and adjust the Serial Device to the device you are using. In this case, *ttyUSB0*. The "Serial port setup" is also where the data channel is configured.

When Minicom is configured with the correct parameters and serial device, it should look like something in Figure 4.4.

4.1.3 Method

The equipment must be configured correctly before commencing the following step. Also, the M-Bus converter must connect the meter device and computer.

Test C.1

In Linux, open the terminal and type:

```
sudo minicom --displayhex
```

This command starts Minicom and converts the output to hex. Minicom will by default output the data it reads from the serial port in ASCII format. Converting it to hex makes it easier to read since the data profile is in hex (see Table 3.1). Enable file capture in Minicom to save the data.

Test C.2

In Linux, open the terminal and type:

```
sudo minicom
```

Commands in Minicom can be called by pressing CTRL-A <key>. To send a file, press "CTRL-A <S>". Minicom gives five different file transfer protocols to use. These are zmodem, ymodem, xmodem, kermit, and ascii. It is possible to send a file after choosing the file transfer protocol. For this test, we used the ASCII file transfer protocol to send a text file 16 bytes and 54,5 kB. We attempted to use the other protocols as well, but this gave us no response from Minicom.

Test C.8

We tried to use the serial link as an interface for shell access to the master meter. If it is possible to upload data to the meter, then we could potentially push commands as well. Minicom can be used to write commands, line by line, which is a tedious process. It can be automated using the Minicom runsript feature. We used a pre-made script by Francesco Robino to obtain shell access [Rob15]. The script can be found in the appendix. To launch the script, type:

```
minicom -C shell_result.txt -S shell_script.txt
```

- -C shell_result.txt: redirect to a file the output of the serial link.
- -S shell_script.txt: executes the script in the .txt file.

4.1.4 Results

Test C.1

The smart meter pushes data on the HAN interface in a given interval. This interval was measured to be one minute, and a data packet of 300 bytes was received for each interval. Below is one of the data packets:

```
37 33 35 39 39 39 32 38 39 31 39 32 32 38 39 34 4b 33 00 00 00 00 00 00 00 00 00
00 00 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```



Figure 4.5: Serial number of the master meter used for testing.

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 09
00 00 00 00 00 00 00 00 00 00 00 83 13 03 ed f9 c0
```

We can map the data received with the data profile provided by Aidon (see Table 3.1). Aidon uses an unsigned data type in little-endian. The first 16 bytes represents the serial number of the meter device:

```
37 33 35 39 39 39 32 38 39 31 39 32 32 38 39 34
```

Using a hex to ASCII converter, we get the number *7359992891922894* which matches the serial number of the meter device used for testing (see Figure 4.5).

The rest of the data have been converted to decimal and is given in Table 4.1. The last three remaining bytes, *ed f9 c0*, are not defined by Table 3.1. If we produce the CRC16-CCITT checksum of the preceding bytes using an online CRC checksum calculator [Bie17], we get *f9 ed*". The checksum calculated matches the first two bytes outside of the data profile (given little-endian). We can, therefore, assume that these two bytes are used for the checksum. The last byte *"c0"* will be discussed in a moment.

To verify the numbers from the master meter, we examined the output from the HAN interface of a slave meter as well. The meter devices are highly similar, but the slave has a different system module installed since it does not communicate with the HES. The data profile is the same for both devices which allows us to compare the data. The slave meter came with a power strip pre-installed (see Figure 4.6) which

Field	Data type	Value
A+	U64	13131
A-	U64	0
R+	U64	6
R-	U64	0
P+	U32	0
P-	U32	0
Q+	U32	0
Q-	U32	0
Phi1	U16	0
Phi2	U16	0
Phi3	U16	0
P1	U32	0
P2	U32	0
P3	U32	0
U1	U16	2314
U2	U16	0
U3	U16	0
I1	U16	0
I2	U16	0
I3	U16	0
F	U16	4995
Phases	U8	3

Table 4.1: Data analyzed from master meter without load.

enabled us to see how numbers change if a load is applied to the meter. When not applying any load we get the following data packet:

```
37 33 35 39 39 39 32 38 39 30 36 35 36 35 31 36 35 12 44 00 00 00 00 00 00 00 00
00 00 00 00 ba 26 12 00 00 00 00 00 00 6a 9b 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
ee 08 00 00 00 00 00 00 00 00 8a 13 03 16 1f c0
```

The first 16 bytes matches the serial number of the slave meter (see Figure 4.7). Table 4.2 shows the remaining data for the data profile after converting it to decimal.

We see that some of the fields from the slave meter differ from the master meter. These fields are A+, R+, R-, and U2. Most likely this is because of the installed



Figure 4.6: Slave meter with power strip installed.



Figure 4.7: Serial number of the slave meter used for testing.

Field	Data type	Value
A+	U64	4461109
A-	U64	0
R+	U64	1189562
R-	U64	39786
P+	U32	0
P-	U32	0
Q+	U32	0
Q-	U32	0
Phi1	U16	0
Phi2	U16	0
Phi3	U16	0
P1	U32	0
P2	U32	0
P3	U32	0
U1	U16	2304
U2	U16	2286
U3	U16	0
I1	U16	0
I2	U16	0
I3	U16	0
F	U16	5002
Phases	U8	3

Table 4.2: Data analyzed from slave meter without load.

power strip. It may also be something to do with the difference between the meter devices. However, U1 (voltage for L1) and F (network frequency) are almost identical between the devices. The calculated CRC16-CCITT checksum is *"1F 16"* which matches the checksum from the reader.

We tried looking at how the numbers change when applying a load to the slave meter. It was applied by attaching a 61-watt laptop charger to the power strip. After applying the load, the numbers change. The new values are listed in Table 4.3. Similar to all readings is the last byte, *"c0"*. Since this is the same between different devices, it is most likely a stop byte. Joar G. Harkestad later confirmed that it is a stop byte. Harkestad is CEO of Hark Technologies, a company which works on a wireless transmitter to send data from the HAN interface of smart meters (including Aidon meters) to the home network.

Field	Data type	Value
A+	U64	4461110
A-	U64	0
R+	U64	1189562
R-	U64	39786
P+	U32	38
P-	U32	0
Q+	U32	0
Q-	U32	73
Phi1	U16	35078
Phi2	U16	0
Phi3	U16	0
P1	U32	38
P2	U32	0
P3	U32	0
U1	U16	2310
U2	U16	2288
U3	U16	0
I1	U16	3
I2	U16	0
I3	U16	0
F	U16	4997
Phases	U8	3

Table 4.3: Data analyzed from slave meter with load.

Test C.2

Minicom indicated that both text files were successfully uploaded, see Figure 4.8 and 4.9. However, we were not able to confirm this.

Test C.8

It was not possible to get shell access on the master meter using the pre-made script. Figure 4.10 shows that the script attempts to log in, but is not successful.

```

henrik@ntnu-kontor: ~
Welcome to minicom 2.7
OPTIONS: I18n
Compiled on Feb 7 2016, 13:37:27.
Port /dev/ttyUSB0, 11:47:17
+-----[ascii upload - Press CTRL-C to quit]-----+
Press CTRL|ASCII upload of "test"
|
| 54.4 Kbytes transferred at 960 CPS... Done.
|
| READY: press any key to continue...|
|
+-----+
CTRL-A Z for help | 9600 8N1 | NOR | Minicom 2.7 | VT102 | Offline | ttyUSB0

```

Figure 4.8: Completed upload of 54,5 kB file to the HAN interface.

```

henrik@ntnu-kontor: ~
Welcome to minicom 2.7
OPTIONS: I18n
Compiled on Feb 7 2016, 13:37:27.
Port /dev/ttyUSB0, 15:00:23
+-----[ascii upload - Press CTRL-C to quit]-----+
Press CTRL|ASCII upload of "fil"
|
| 0.0 Kbytes transferred at 17 CPS... Done.
|
| READY: press any key to continue...|
|
+-----+
CTRL-A Z for help | 9600 8N1 | NOR | Minicom 2.7 | VT102 | Offline | ttyUSB0

```

Figure 4.9: Completed upload of 16 byte file to the HAN interface. Note that it says 0.0 Kbytes transferred because of the small file size.


```

henrik@ntnu-kontor: ~
Welcome to minicom 2.7

OPTIONS: I18n
Compiled on Feb 7 2016, 13:37:27.
Port /dev/ttyUSB0, 11:29:11

Press CTRL-A Z for help on special keys

Trying to Login..
█

```

Figure 4.10: Attempted login using the HAN interface.

4.2 Test C.3, C.4, and C.8

4.2.1 Equipment

- Computer
- Aidon 6550 smart meter with Aidon 6478 system module
- RS232 cable
- Minicom 2.7 (or any other serial port communications program)

Four components are used to communicate with the RS232 interface. First of is the smart meter with a system module that supports the RS232 interface. A desktop computer running Ubuntu 16.04 operating system is used to run relevant software for the test. Minicom is used to read data from the RS232 interface and send data. An RS232 cable is used to connect the meter and computer

4.2.2 Setup

Some of the details for the setup are similar as for testing the HAN interface. We have therefore made a more compact version to reduce redundant information. Among others, details on how to identify the correct serial interface to listen on in Minicom has been excluded.

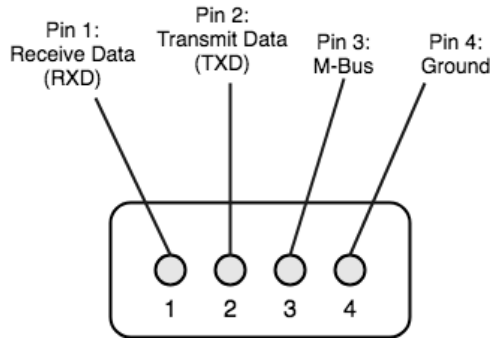


Figure 4.11: Layout of the 4-pin connector on the smart meter.

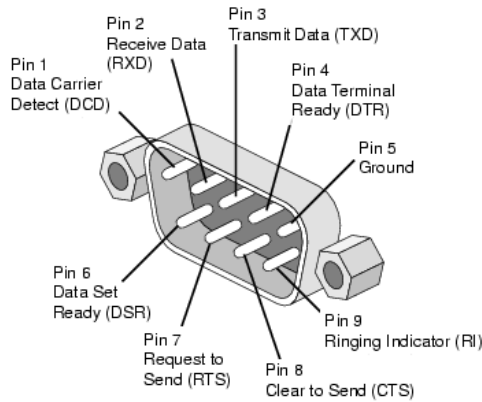


Figure 4.12: Layout of the RS232 serial port head [Gro01].

Aidon has a 4-pin connector used for the RS232 and HAN interface. The connector is found on two system modules, namely the Aidon 6478 Master and Aidon 6484 Slave. Figure 4.11 illustrates the layout of the 4-pin connector on the meter. This layout was obtained from Aidon and by analyzing a RS232 cable which was bundled with the smart meter. From Aidon’s documentation, we know that pin 3 is used for the M-Bus signal, and that pin 4 is Ground. We saw that the pin 1 matched the Receive Data (RXD) pin, and that pin 2 matched the Transmit Data (TXD) pin, by comparing the provided RS232 cable with the RS232 serial interface. Figure 4.12 illustrates the pins on the RS232 serial port head. The RS232 interface on the system module uses pin 2, 3, and 5 from Figure 4.12. In Figure 4.11, this corresponds to pin 1, 2, and 4. We created a new RS232 cable by soldering three wires to a RS232 serial port head using the identified mapping. Figure 4.13 shows the cable.

The RS232 cable was connected to the appropriate pins on the smart meter

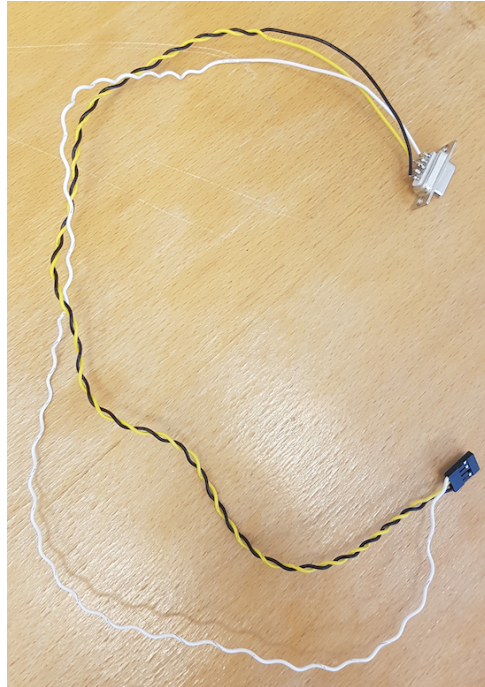


Figure 4.13: RS232 cable used to connect with the smart meter.

and the computer's serial interface connection. To communicate with the RS232 interface, Minicom needs to be configured for the correct data channel. Aidon uses the following parameters in the configuration of the data channel:

- Baud rate: 115200 bps
- 8 data bits
- No parity
- One stop bit

We need to configure Minicom to use the correct serial interface, in this case, the *ttyS0* interface. Figure 4.14 show the final configuration of the data channel.

4.2.3 Method

The equipment must be configured correctly before commencing the following steps. Also, make sure that the RS232 cable is attached to the correct pins on the smart meter.

```

henrik@ntnu-kontor: ~
Welcome to minicom 2.7

OPTI+-----+
Comp| A - Serial Device      : /dev/ttyS0
Port| B - Lockfile Location  : /home/henrik/Documents/Minicom
    | C - Callin Program     :
Pres| D - Callout Program    :
    | E - Bps/Par/Bits       : 115200 8N1
    | F - Hardware Flow Control : No
    | G - Software Flow Control : No
    |
    | Change which setting? |
+-----+
    | Screen and keyboard  |
    | Save setup as dfl   |
    | Save setup as..    |
    | Exit                 |
+-----+

CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.7 | VT102 | Offline | ttyS0

```

Figure 4.14: Configuration of the data channel for the RS232 interface

Test C.3

In Linux, open the terminal and type:

```
sudo minicom
```

This command starts Minicom which will read data from the interface. Minicom will by default output the data in ASCII format. This worked well for this test since data was sent in ASCII format. Enable file capture in Minicom to save the data.

Test C.4

In this test, we used the same method as for test C.2. We only attempted to upload the 54,5 Kb file. Uploading a smaller file should not affect the results.

Test C.8

We used the same method as for the HAN interface. To launch the script, enter:

```
minicom -C shell_result.txt -S shell_script.txt
```

4.2.4 Results

Test C.3

The smart meter continually pushes data on the RS232 interface, but consumption data was only pushed at a fixed interval. This interval was measured to be one minute. A snippet of the consumption data is displayed in Figure 4.15. From the snippet, we can see that the network frequency and voltage match the values obtained from the HAN interface reading.

There was additional information pushed from the interface. The only part we considered interesting was:

```
INFO: 2018-01-22 17:13:45: no encryption defined with info=0
```

We assume this means that no encryption is used for information pushed from the RS232 interface.

Test C.4

Minicom indicated that the text file was successfully uploaded (see Figure 4.16). However, we were not able to confirm this. The additional information displayed is noise from the continual data readings.

Test C.8

It was not possible to get shell access on the master meter using the pre-made script. Figure 4.17 shows that the script attempts to login but is not successful. The additional information displayed is noise from the continual data readings.

4.3 Test C.5

4.3.1 Equipment

- Computer (with Ethernet connection)
- isc-dhcp-server (v. 4.3.3)
- Wireshark (v. 2.2.6)
- Netcat (v. 1.105)
- Nmap (v. 7.01)

```

ENHANCED: 2018-01-22 17:13:06: ENWQ: Froze datarecord:
timestamp 569956320
status 0028
network frequency 5001
max eaf current 0
avg eaf current 0
A+ 0
A- 0
R+ 0
R- 0
phase 1:
valid periods 4
missing periods 0
avg current 0
max current 0
max current time 0
max current voltage 0
avg voltage 2328
max voltage 2329
max voltage time 0
min voltage 2327
min voltage time 16
3rd harmonic voltage 10
5th harmonic voltage 15
7th harmonic voltage 11
voltage THD 119
voltage slope 1
phase 2:
valid periods 0
missing periods 4
avg current 0
max current 0
max current time 0
max current voltage 0
avg voltage 0
max voltage 0
max voltage time 0
min voltage 9999
min voltage time 0
3rd harmonic voltage 0
5th harmonic voltage 0
7th harmonic voltage 0
voltage THD 0
voltage slope 0
phase 3:
valid periods 0
missing periods 4
avg current 0
max current 0
max current time 0
max current voltage 0
avg voltage 0
max voltage 0
max voltage time 0
min voltage 9999
min voltage time 0
3rd harmonic voltage 0
5th harmonic voltage 0
7th harmonic voltage 0
voltage THD 0
voltage slope 0

```

Figure 4.15: Consumption data from the RS232 reading

```

henrik@ntnu-kontor: ~
INFO: 2018-05-31 s
4
d
1
%
0
S
0
0
5
S
1
%
8
S
k
:
1
1
0
S
r
0
+-----[ascii upload - Press CTRL-C to quit]-----+
|1|
|INFO: 2018-05-31 12:38:01: cron: pending 3500 ms|
|37.8 Kbytes transferred at 9671 CPSENHANCED: 2018-05-31 12:38|
|:02: error active: 20:8000|
|54.4 Kbytes transferred at 11144 CPS... Done.|
|
| READY: press any key to continue...|
+-----+
CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.7 | VT102 | Offline | ttyS0

```

Figure 4.16: Completed upload of 54,5 Kb file to the RS232 interface.

```

henrik@ntnu-kontor: ~
Welcome to minicom 2.7
OPTIONS: I18n
Compiled on Feb 7 2016, 13:37:27.
Port /dev/ttyS0
Press CTRL-A Z for help on special keys
Trying to Login..
MAINTAIN: 2018-06-02 11:36:01: meter reader cache: no hit for 21.7.0
cache hit r%
0
4
S
k
5
S
:
0
8
6

```

Figure 4.17: Attempted login using the RS232 interface

A computer was used to run the DHCP server and to communicate with the meter device using terminal commands. The DHCP server software used is called `isc-dhcp-server` (open source DHCP software system) [McN15]. Wireshark was used to analyze the network traffic. Netcat was used for active communication between the meter and computer. Nmap was used to map all the open ports on the meter.

4.3.2 Setup

In this test, we want to perform a MITM attack between the master meter and HES using Ethernet for communication. It should not matter what communication technology is used if we want to inspect data on the application layer. Performing a MITM attack over Ethernet reduces the setup time compared to configuring an IMSI catcher. It is, therefore, the preferred method since the results achieved are believed to be the same. To clarify this, the transport medium used between the master meter and HES should not affect the content of the payload. The goal of the MITM attack is to see if we can sniff traffic from the meter, or in some way communicate with it.

The setup for this test is separated into three stages:

1. Install `isc-dhcp-server`.
2. Configure subnet for DHCP server.
3. Configure network interface.

Install `isc-dhcp-server` To set up the attack, we need to configure the computer in such a way that it can communicate with the meter. An easy way to do this is to install `isc-dhcp-server` on a computer and connect the meter directly to the wired network interface (Ethernet). *DHCP is a network service that enables host computers to be automatically assigned settings from a server as opposed to manually configuring each network host.* [McN15]. The computer will work as a server and automatically assign network configurations, such as the IP address, to the meter device. Assigning network configurations to the meter will allow it to communicate to the local network and we can intercept the traffic.

To install `isc-dhcp-server` on Ubuntu, open the Linux terminal and enter:

```
sudo apt-get install isc-dhcp-server
```

Configure subnet for DHCP server Once installed, we need to configure a subnet for the DHCP server. `isc-dhcp-server` comes with a default configuration file called `dhcpd.conf` where this can be configured. To access the file, enter the following in the terminal:


```
nano -w /etc/dhcp/dhcpd.conf
```

The first configuration of dhcpd.conf used for testing was:

```
option domain-name "test.no";
option domain-name-servers 8.8.8.8, 8.8.4.4;

default-lease-time 600;
max-lease-time 7200;

ddns-update-style none;

subnet 10.100.100.1 netmask 255.255.255.0 {
    range 10.100.100.1 10.100.100.254;
    option routers lol.test.no;
}
```

Configure network interface After installing isc-dhcp-server and configuring the DHCP server, we have to:

- Configure the network interface.
- Identify the correct interface to connect the meter.
- Assign an IP address to the interface and a subnet which matches the one set for the DHCP server.

Assigning an IP address to the interface was done using:

```
sudo ifconfig enp13s0 10.100.100.1 netmask 255.255.255.0
```

10.100.100.1 is the IP address we assigned to the interface. isc-dhcp-server will automatically use it as an IP address for the DHCP server, but it can also be used to communicate with the meter. The netmask defines the range of IP addresses on the interface. A netmask of 255.255.255.0 leaves us with 8 bits which can be used for 256 different IP addresses. The netmask assigned to the interface should match the one set in the dhcpd.conf file.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	350	DHCP Discover - Transaction ID 0xabcd0001
2	0.998324	IntelCor_87:08:c6	Broadcast	ARP	42	Who has 10.100.184.20? Tell 10.100.184.1
3	1.003475	10.100.184.1	10.100.184.20	DHCP	342	DHCP Offer - Transaction ID 0xabcd0001
4	1.003736	0.0.0.0	255.255.255.255	DHCP	350	DHCP Request - Transaction ID 0xabcd0002
5	1.036102	10.100.184.1	10.100.184.20	DHCP	342	DHCP ACK - Transaction ID 0xabcd0002
6	1.036217	00:00:00:00:00:00	Broadcast	ARP	60	Who has 10.100.184.20? Tell 0.0.0.0
7	1.499969	00:00:00:00:00:00	Broadcast	ARP	60	Who has 10.100.184.20? Tell 0.0.0.0
8	1.998321	IntelCor_87:08:c6	Broadcast	ARP	42	Who has 10.100.184.20? Tell 10.100.184.1
9	17.498764	00:00:00:00:00:00	Broadcast	ARP	60	Who has 10.100.184.1? Tell 10.100.184.20
10	17.498787	IntelCor_87:08:c6	00:00:00:00:00:00	ARP	42	10.100.184.1 is at 00:1b:21:87:08:c6
11	17.499022	10.100.184.20	10.100.184.169	TCP	60	49153 -> 4002 [SYN] Seq=0 Win=1024 Len=0 MSS=256
12	20.248106	10.100.184.20	10.100.184.169	TCP	60	[TCP Retransmission] 49153 -> 4002 [SYN] Seq=0 Win=1024 Len=0 MSS=256
13	22.492349	10.100.184.1	224.0.0.251	MDNS	183	Standard query 0x0000 PTR _nfs._tcp.local, "QM" question PTR _inp._t
14	23.248221	10.100.184.20	10.100.184.169	TCP	60	[TCP Retransmission] 49153 -> 4002 [SYN] Seq=0 Win=1024 Len=0 MSS=256
15	95.460991	10.100.184.20	10.100.184.169	TCP	60	49154 -> 4002 [SYN] Seq=0 Win=1024 Len=0 MSS=256
16	98.460195	10.100.184.20	10.100.184.169	TCP	60	[TCP Retransmission] 49154 -> 4002 [SYN] Seq=0 Win=1024 Len=0 MSS=256
17	101.459955	10.100.184.20	10.100.184.169	TCP	60	[TCP Retransmission] 49154 -> 4002 [SYN] Seq=0 Win=1024 Len=0 MSS=256
18	104.459925	10.100.184.20	10.100.184.169	TCP	60	[TCP Retransmission] 49154 -> 4002 [SYN] Seq=0 Win=1024 Len=0 MSS=256
19	107.460017	10.100.184.20	10.100.184.169	TCP	60	[TCP Retransmission] 49154 -> 4002 [SYN] Seq=0 Win=1024 Len=0 MSS=256
20	110.460042	10.100.184.20	10.100.184.169	TCP	60	[TCP Retransmission] 49154 -> 4002 [SYN] Seq=0 Win=1024 Len=0 MSS=256

Figure 4.18: First packet capture from the master meter using 10.100.100.1 as IP for the interface.

4.3.3 Method

Sniff data

Once the DHCP server and interface have been configured, we can listen to traffic. It is recommended to disconnect the meter device from the computer, restart the DHCP server, and reset the interface, to reduce issues for the test.

Restart of DHCP server:

```
sudo /etc/init.d/isc-dhcp-server restart
```

Restart of interface:

```
sudo ifconfig enp13s0 10.100.100.1 netmask 255.255.255.0
```

To capture data from the interface, enter the command:

```
sudo tcpdump -vv -i enp13s1 -w <file-name>
```

tcpdump is a command line tool which lets us capture and analyze incoming and outgoing traffic on an interface. *-vv* defines how detailed data we want from the capture. *-i* defines what interface we want to listen to. In our case, the meter is connected to the interface *enp13s1*. *-w* allows us to capture the data and write it to a file. For *<file-name>* you can enter the name of what you want to call the dump of data. It will be saved as a *.cap* file which we can inspect in Wireshark.

Figure 4.18 shows the first *tcpdump* we inspected in Wireshark.

It is required to have some knowledge of network communication to understand the traffic in Wireshark. We will cover some concepts relevant to understand the data captures.

DHCP: DHCP consists of four steps: DHCP Discovery, DHCP Offer, DHCP Request and DHCP Acknowledgement.

1. **DHCP Discovery:** The DHCP Discover message is an IP lease request. When a device connects to a network, the first packet it will send out is a broadcast message, known as DHCP Discover. The intention is to notify the DHCP server that it has connected to the network and wants to be assigned an IP address.
2. **DHCP Offer:** The DHCP server reserves an IP address for the client and makes a lease offer by sending a DHCP Offer message to the client. The message contains the client's MAC address, the IP address which has been reserved for the client, the subnet mask, the duration of the lease, and the IP address of the DHCP server making the offer.
3. **DHCP Request:** When the client receives a DHCP Offer with an IP address, it replies with a DHCP Request, requesting the offered address. Since there can be multiple DHCP servers offering an IP address, the client has to pick one of them. Servers will be informed whose offer the client has accepted. Offers that are not accepted are withdrawn.
4. **DHCP ACK:** The DHCP server which receives the DHCP Request replies with a DHCP ACK back to the client. This message contains, among others, the leasing period of the IP address and any other configuration information that the client might have requested. The IP configuration is now completed.

When inspecting the tcpdump, we see the four stages of the DHCP protocol between the meter and the DHCP server. Note that the IP address of the meter is 0.0.0.0 before an IP address have been assigned to it. After the four phases have completed, the meter is given the IP address 10.100.100.2.

What is interesting is that the meter tries to connect to the IP address 10.100.184.169 on port 4002. This address is out of range for the subnet that was defined in dhcpd.conf. We can listen to the traffic on the address by changing the subnet in the file such that the address is in range. dhcpd.conf will look like this then:

```
option domain-name "test.no";
option domain-name-servers 8.8.8.8, 8.8.4.4;

default-lease-time 600;
```

```
max-lease-time 7200;

ddns-update-style none;

subnet 10.100.184.1 netmask 255.255.255.0 {
    range 10.100.184.1 10.100.184.254;
    option routers lol.test.no;
}
```

There are some further settings we have to change. These changes are the address of the DHCP server, and netmask of the interface to match the newly defined subnet.

```
sudo ifconfig enp13s0 10.100.184.1 netmask 255.255.255.0
```

Furthermore, we want to add the address *10.100.184.169* to the interface such that we can use Netcat to listen for incoming traffic on that address. Netcat is a software which can be used to read and write to network connections using TCP or UDP. To add the new address 10.100.184.169, enter:

```
sudo ifconfig enp13s0:2 10.100.184.169 netmask 255.255.255.0
```

Reset the DHCP server and replug the smart meter. The new data capture is displayed in Figure 4.19. The meter has now been given the IP address 10.100.184.2 and is trying to establish a TCP connection with the IP address 10.100.184.169, which we have assigned to our interface enp13s1. TCP uses a three-way handshake to establish a TCP connection. A successful three-way handshake consists of the following steps:

1. **SYN:** The initiator sends a SYN to the server.
2. **SYN-ACK:** The recipient replies with a SYN-ACK.
3. **ACK** The initiator replies with an ACK.

10.100.184.169 responds with a [RST, ACK] because we are not currently listening for traffic on port 4002 (port which the meter attempts to connect to).

If we use Netcat, we can listen for traffic on port 4002 to establish a TCP connection and inspect the data sent. To use Netcat to listen for traffic on port 4002, enter the following in the terminal:

```
sudo nc -lnvp 4002
```

1	0.000000	0.0.0.0	255.255.255.255	DHCP	350	DHCP Discover	- Transaction ID 0xabcd0001
2	0.002622	10.100.184.1	10.100.184.2	DHCP	342	DHCP Offer	- Transaction ID 0xabcd0001
3	0.002957	0.0.0.0	255.255.255.255	DHCP	350	DHCP Request	- Transaction ID 0xabcd0002
4	0.003108	10.100.184.1	10.100.184.2	DHCP	342	DHCP ACK	- Transaction ID 0xabcd0002
5	0.003428	00:00:00:00:00:00	Broadcast	ARP	60	Who has 10.100.184.2?	Tell 0.0.0.0
6	0.499949	00:00:00:00:00:00	Broadcast	ARP	60	Who has 10.100.184.2?	Tell 0.0.0.0
7	0.964263	10.100.184.1	224.0.0.251	MDNS	183	Standard query 0x0000 PTR _nfs._tcp.local,	"QM"
8	10.398814	00:00:00:00:00:00	Broadcast	ARP	60	Who has 10.100.184.1?	Tell 10.100.184.2
9	10.398841	IntelCor_87:08:c6	00:00:00:00:00:00	ARP	42	10.100.184.1 is at	00:1b:21:87:08:c6
10	10.399061	10.100.184.2	10.100.184.169	TCP	60	49153 → 4002 [SYN]	Seq=0 Win=1024 Len=0 MSS=256
11	10.399087	10.100.184.169	10.100.184.2	TCP	54	4002 → 49153 [RST, ACK]	Seq=1 Ack=1 Win=0 Len=0
12	15.404259	IntelCor_87:08:c6	00:00:00:00:00:00	ARP	42	Who has 10.100.184.2?	Tell 10.100.184.1
13	15.404545	00:00:00:00:00:00	IntelCor_87:08:c6	ARP	60	10.100.184.2 is at	00:00:00:00:00:00
14	16.980889	10.100.184.1	224.0.0.251	MDNS	183	Standard query 0x0000 PTR _nfs._tcp.local,	"QM"

Figure 4.19: Second packet capture from the master meter using 10.100.184.1 and 10.100.184.169 as IP for the interface.

1	0.000000	10.100.184.2	10.100.184.169	TCP	60	49232 → 4002 [SYN]	Seq=0 Win=1024 Len=0 MSS=256
2	0.000042	10.100.184.169	10.100.184.2	TCP	58	4002 → 49232 [SYN, ACK]	Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
3	0.000156	10.100.184.2	10.100.184.169	TCP	60	49232 → 4002 [ACK]	Seq=1 Ack=1 Win=1024 Len=0
4	0.141375	10.100.184.2	10.100.184.169	TCP	80	49232 → 4002 [PSH, ACK]	Seq=1 Ack=1 Win=1024 Len=26 [TCP segment of a reassembled PDU]
5	0.141402	10.100.184.169	10.100.184.2	TCP	54	4002 → 49232 [ACK]	Seq=1 Ack=27 Win=29200 Len=0
6	30.141436	10.100.184.2	10.100.184.169	TCP	60	49232 → 4002 [FIN, ACK]	Seq=27 Ack=1 Win=1024 Len=0
7	30.141558	10.100.184.169	10.100.184.2	TCP	54	4002 → 49232 [FIN, ACK]	Seq=1 Ack=28 Win=29200 Len=0
8	30.141654	10.100.184.2	10.100.184.169	TCP	60	49232 → 4002 [ACK]	Seq=28 Ack=2 Win=1023 Len=0

Figure 4.20: Third packet capture from the master meter using 10.100.184.1 and 10.100.184.169 as IP for the interface. Netcat is used to listen for traffic on port 4002 and establish a TCP connection.

Netcat will listen to incoming traffic on all IP addresses for port 4002. "nc" is the abbreviation for Netcat, -lnvp are options for the Netcat command, and 4002 is the port we want to listen on. The following explanation of the options are taken from a Netcat Cheat Sheet found online [Ins18]:

- -l: Listen mode (default is client mode).
- -n: Don't perform DNS lookups on names of machines on the other side.
- -v: Be verbose, printing out messages on Standard Error, such as when a connection occurs.
- -p: Local port (In listen mode, this is port listened on. In client mode, this is source port for all packets sent).

Figure 4.20 shows the new data captured where the meter establish a TCP connection with 10.100.184.169.

After the connection have been established, the meter sends a data packet. Let us call this packet nr. 1:

```
55 aa 01 be ba 13 00 01 4e 19 5a bb 1e 04 b2 20
03 02 2c 01 7c 00 00 01 00 00
```

The meter closes the TCP connection after the first packet is sent. Thereafter, it re-establishes a TCP connection with 10.100.184.169 and sends an almost identical packet. Let us call this packet nr. 2:

```
55 aa 01 be ba 13 00 01 4e 19 5a bb 1e 04 b2 20
03 02 2c 01 7c 00 5b 06 00 00
```

The two messages only differ by two bytes, which have been highlighted. The meter re-establishes a TCP connection between all consecutive packets received. These packets have the same format as packet nr. 2.

To check for consistency, we restarted the meter and performed a new packet capture five times. The following pattern emerged. If we restart the meter, then message nr. 1 is sent. For all consecutive transmissions, then message nr. 2 is sent.

Transmit data

We can use the open source security software Nmap [Lyo18] to search for open ports on the IP address of the meter (10.100.184.2). Nmap will try to establish a TCP connection with all the ports for the specified IP address. If the port is open, the recipient will accept the connection. Nmap will give you a list of all the ports it established a connection with. To use Nmap on the IP address of the meter, type the following command in terminal:

```
nmap 10.100.184.2
```

The result from running nmap is that only port 9999 is open on the meter, see Figure 4.21.

Let us try to connect to the port using Netcat. Note that the connection is established from IP 10.100.184.1 on the interface. The command to connect is:

```
nc 10.100.184.2 9999
```

When trying to connect, the TCP connection is established and the meter sends the following message back to 10.100.184.1:

```
55 aa 01 be ba 13 00 01 4e 19 5a bb 1e 04 b2 20
03 02 2c 01 7c 00 5b 06 00 00
```

```

Starting Nmap 7.01 ( https://nmap.org ) at 2018-05-03 14:10 CEST
Nmap scan report for 10.100.184.2
Host is up (0.00023s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
9999/tcp  open  abyss
MAC Address: 00:00:00:00:00:00 (Xerox)

```

Figure 4.21: Nmap is used to scan for open ports on the meter. Only port 9999 is confirmed open after the test.

12	15.126995	10.100.184.1	10.100.184.2	TCP	74	60526	→	9999	[SYN]	Seq=0	Win=29200	Len=0	MSS=1460	SA=10.100.184.1	DA=10.100.184.2
13	15.126995	10.100.184.2	10.100.184.1	TCP	66	9999	→	60526	[SYN, ACK]	Seq=9	Ack=1	Win=1024	Len=0	SA=10.100.184.2	DA=10.100.184.1
14	15.127027	10.100.184.1	10.100.184.2	TCP	54	60526	→	9999	[ACK]	Seq=1	Ack=1	Win=29200	Len=0	SA=10.100.184.1	DA=10.100.184.2
15	15.127093	10.100.184.1	10.100.184.2	TCP	87	60526	→	9999	[PSH, ACK]	Seq=1	Ack=1	Win=29200	Len=33	SA=10.100.184.1	DA=10.100.184.2
16	15.127133	10.100.184.1	10.100.184.2	TCP	54	60526	→	9999	[FIN, ACK]	Seq=34	Ack=1	Win=29200	Len=0	SA=10.100.184.1	DA=10.100.184.2
17	15.127250	10.100.184.2	10.100.184.1	TCP	60	9999	→	60526	[ACK]	Seq=1	Ack=35	Win=990	Len=0	SA=10.100.184.2	DA=10.100.184.1
19	27.221421	10.100.184.2	10.100.184.1	TCP	80	9999	→	60526	[PSH, ACK]	Seq=1	Ack=35	Win=990	Len=26	SA=10.100.184.2	DA=10.100.184.1
20	27.221451	10.100.184.1	10.100.184.2	TCP	54	60526	→	9999	[ACK]	Seq=35	Ack=27	Win=29200	Len=0	SA=10.100.184.1	DA=10.100.184.2
21	27.221400	10.100.184.2	10.100.184.1	TCP	60	9999	→	60526	[RST, ACK]	Seq=27	Ack=35	Win=1024	Len=0	SA=10.100.184.2	DA=10.100.184.1
22	27.221578	10.100.184.2	10.100.184.1	TCP	60	9999	→	60526	[RST, ACK]	Seq=27	Ack=35	Win=1024	Len=0	SA=10.100.184.2	DA=10.100.184.1

Figure 4.22: Analysis of network traffic in Wireshark when sending data to the meter.

This message is identical to message nr. 2 which was sniffed from the meter earlier.

We can also try to send data to the meter using Netcat. For this, we have created a random 33 bytes long text file called "test.txt". The file was sent using the command:

```
nc 10.100.184.2 9999 < test.txt
```

Figure 4.22 displays the traffic between the computer (10.100.184.169) and the meter (10.100.184.2). The file is sent to the meter, but no ACK is received. After the file has been sent, the computer sends a [FIN, ACK] indicating that it wants to terminate the session. The meter then sends a message to the computer which is identical to message nr. 2. The computer responds with an ACK to the received data. However, it looks like this ACK is not received by the meter since it returns a [RST, ACK]. The [RST, ACK] is usually the reply you get when the port is closed, meaning the meter has terminated the session. We tried uploading a bigger file (30 kB), but the response was the same.

4.3.4 Results

Sniffing data

When sniffing data, we noticed that the meter attempts to connect to the static IP address 10.100.184.169, even if the IP is not a part of its subnet. There were two different payloads sent from the meter. The first message sent after reboot is:

```
55 aa 01 be ba 13 00 01 4e 19 5a bb 1e 04 b2 20
03 02 2c 01 7c 00 00 01 00 00
```

The consecutive messages sent afterwards are:

```
55 aa 01 be ba 13 00 01 4e 19 5a bb 1e 04 b2 20
03 02 2c 01 7c 00 5b 06 00 00
```

The period between each re-transmission was measured to be around one minute. Both messages are 26 bytes long, but byte nr. 23 and 24 differ between the first message and the rest. The re-transmission period of one minute is the same frequency as consumption data was pushed from the HAN and RS232 interface. We tried to convert the hex data to ASCII and decimal format but found no correlation between the data from the Ethernet interface and the local communication interfaces.

Transmitting data

It is possible to connect and send data to the meter. However, when sending data to the meter, it does not reply with an ACK. The lack of an ACK response suggests that some filtering mechanism drops the incoming packets. Every time we connect to the meter or attempt to send data to the meter, it replies with the same message as was earlier intercepted:

```
55 aa 01 be ba 13 00 01 4e 19 5a bb 1e 04 b2 20
03 02 2c 01 7c 00 5b 06 00 00
```


Chapter 5

Discussion

In this chapter, we will discuss the results from the testing, how they relate to the research question for this thesis, explanation of unexpected results, and limitations or improvements that could be made to the research.

5.1 HAN interface

5.1.1 Sniffing data

The readings from the HAN interface confirms that data is being transmitted unencrypted. The implications are that whoever obtains data from the interface can read it, given that he knows the format. There are two ways the attacker can gain knowledge of the format. One way is to obtain the data profile. Another way is to obtain different readings from the HAN interface and draw logical conclusions on what the numbers represent. It should be considered a trivial task to decode data from the HAN interface. The implication of having unencrypted data is that customers' consumption data can be exposed to unwanted persons. This is not an immediate threat if the HAN interface is not active or sending data to any devices. However, there are two factors which may affect the exposure of the data. The first factor is the location of where the smart meters are physically installed. If an apartment complex has insufficient physical security of their smart meters, then unwanted persons can access the device and read the data. The second factor is the use of third-party equipment to send the data from the HAN interface to other devices. If data from the HAN interface is accessible through the home network or any third party device, then the potential attack vectors increase.

5.1.2 Uploading files

In Section 2.3 we listed the protocol stack of the Home Area Network (HAN) interface. Among the protocols, we see that the EN 13757-2 standard (M-bus physical layer) is used. According to the EN 13757-2 standard, slave meters can transmit data to

a master meter. In our test setup, the smart meter was the M-Bus master, and the M-Bus converter was a slave device. It is, therefore, theoretically possible to send data to the meter. However, the EN 62056-7-5 standard specifies unidirectional link layer communication on the HAN interface by the default configuration. It should, therefore, only be possible to read data from the interface. There are two possible explanations for why Minicom reported the data to be successfully sent. The first explanation is that the meter just dropped the data it received. The second explanation is that the meter is not using the default configuration of the EN 62056-7-5 standard and accepts incoming data. When comparing the transfer speed for the HAN and RS232 interface, we see that RS232 has a higher transfer speed. On the RS232 interface, we were able to transfer at 11144 Characters Per Second (CPS), while on the HAN interface we were able to transfer at 960 CPS. The difference in transfer speed could further prove that it is possible to send data to the meter. If it is possible to upload data to the meter, then a person could potentially upload malicious files or commands to exploit it. We did not have access to the internal storage of the meter and could, therefore, not confirm if the file was uploaded successfully.

The test could be improved by attempting to upload bigger files. This could potentially generate some error or unexpected results from the smart meter to analyze.

5.1.3 Shell access

It was not possible to get shell access on the master meter using the UNIX login script. Aidon has not confirmed that the meter is running an UNIX operating system, but we made a guess because of its widespread use. Running other types of scripts could be possible, but we did not attempt this. The test could be improved by attempting to run different scripts on the meter.

5.1.4 Symmetric key management

The HAN interface is not standardized in Norway yet, but a security solution is in development. As of today, the government does not impose any requirement for the HAN interface, besides that it must be deactivated upon installation and activated before usage [AS17]. It is troublesome for producers to implement security to the interface if the finalized standard requires the producers to discard current investments in HAN port security. The suggested cryptographic implementation by Norwegian Electrotechnical Committee (NEK) includes the use of symmetric keys to secure the traffic from the HAN interface. Symmetric key algorithms use the same cryptographic key to encrypt and decrypt data. A challenge with symmetric key encryption is that it requires a key management system to generate, distribute,

store, use, destroy and replace keys. OWASP have published a "cheat sheet" on how to achieve the functionality in a secure way [OWA17]. Although OWASP focuses on web application security, their recommendations can be considered applicable in other security systems as well. The recommendations below are based on the recommendations from OWASP [OWA17].

Key management recommendations

It is important to generate strong keys such that the security of the data is not undermined by weak cryptographic keys. The strength of the key is a combination of sufficient key length and randomness. What is "sufficient", is determined by the data security requirements. The data from the HAN port is considered personal data, thereby regulated by the Personal Data Act (PDA). This should be reflected in the security requirements. Generation of keys should not be predictable to avoid that an attacker can easily guess the correct key. That is, the key data should have high entropy (randomness). Key distribution must be secured to avoid theft of encryption keys. The most secure way is to use an existing encryption channel. The security of the channel depends on the security of a previous key exchange used to establish the channel. Aidon have implemented an extensive key hierarchy which could be utilized for this. Another alternative is to use some sort of public key cryptography to create the secure channel. Diffie Hellman could help secure the distribution of keys. The use of secure transport such as TLS and SSHv2 can also secure the keys in transit. Storage of keys should be done using a strong access control, auditing, and logging for the keys. Access to encryption keys should be allowed to the smallest amount of people at the HES. They should further be non-attainable for the customers. Aidon is using a "keystore" to store cryptographic keys. The keys are encrypted using Key Encryption Keys (KEKs). Encryption keys on the smart meter stored on the internal flash are read protected. Aidon provides security logs of occurring events during the processing of an inbound or outbound message between the meter and HES. It is not known if they provide logging or auditing of stored keys in the HES. An issue to consider is how long time a key is to be used. To increase the required effort for an attacker to obtain a key, they should be frequently replaced. The resources spent to replace a key must be considered against the security requirement for the keys. This will dictate how often the keys are replaced. An example of replacement policy is the Payment Card Industry Data Security Standard (PCI DSS). The standard mandates that keys used for encryption of credit card data must be rotated at least annually. Aidon already have a key management system in place which would need to incorporate the symmetric keys in a secure way. Compromised keys should be destroyed and replaced securely. This is covered by the processes involved with distribution, storage and replacement of keys.

5.1.5 Activation of HAN port

The proposed security solution to the HAN interface suggests that the interface is only activated if the customers request it. When a customer requests activation, sufficient security will be offered by encrypting traffic and ensuring the physical security of the meter (provided by customer or Distribution Network Operator (DSO)). The activation process includes a key exchange. The question is what does it mean for the interface to be activated? As of now, when the current in the line loop exceeds 10 mA (a device is connected), the data flow is activated, and a fixed data set is sent every minute [Aid15]. If this continues to be the default configuration, then a customer could use the interface without requesting it to be activated. It could counteract the use of symmetric keys for encryption because the user (or an attacker) can circumvent the security solution. The prerequisite is that encryption is only applied when the HAN interface is activated. Note that the smart meter used for testing in this thesis may differ from the one supplied to customers.

5.2 RS232 interface

It was confirmed by Rolf Pedersen that the RS232 interface is activated for the meter device lent to NTNU, but that it is not active for customers. It is not possible to communicate with the RS232 interface if the interface is not activated. We do not have access to a meter installed at a customer and can therefore not test this claim. We could have exploited our meter to gain information about other security configurations in the meter. However, we were not successful. Because the interface is supposedly not active for customers, we consider it not relevant to discuss the results of the testing further.

5.3 MITM attack

5.3.1 RADIUS issues

When listening to traffic from the meter using the Ethernet interface, the meter sends the same message every time. The reason why the meter keeps re-transmitting the same messages is that it attempts to connect with the Head End System (HES) using the Remote Authentication Dial-In User Service (RADIUS) authentication protocol [Ped18]. It is unclear why the first packet differs from the rest. It could be that re-transmitted messages are marked using two bytes.

The RADIUS protocol with the PAP authentication scheme has some vulnerabilities which are caused by the protocol, or by a bad implementation which is exacerbated by the protocol. Many of the vulnerabilities are caused by the use of MD5 to protect the User-Password attribute. They can be mitigated using a secure

channel for communication. We did not have access to the meteringware (used in the HES) nor encryption keys, which would possibly allow us to complete the RADIUS authentication and analyze the process. Also, Aidon has not confirmed which authentication scheme they use for RADIUS authentication. It is likely that Aidon use CHAP because they have an extensive key hierarchy. However, we consider it relevant to cover some of the vulnerabilities since Aidon is using the RADIUS protocol.

Response Authenticator Based Shared Secret Attack

An attacker can execute an exhaustive off-line attack on the shared secret by intercepting a valid Access-Request and the associated Access-Accept packet. The attacker can pre-compute the MD5 state for (Code|ID|Length|RequestAuth|Attributes), and resume it once for each shared secret guess. If the attacker has guessed the correct shared secret, then the MD5 calculation will be the same as the ResponseAuth in the Access-Accept message.

User-Password Attribute Based Shared Secret Attack

The User-Password attribute is protected using a stream cipher. An attacker can exploit this by observing the network traffic and attempt authentication. First, the attacker attempts to authenticate with a known password, and initiate the authentication process. The client will produce an Access-Request packet which it sends to the server. The attacker captures this packet and XOR the protected portion of the User-Password attribute with the password he provided to the client. This process gives the value of the MD5(Shared Secret + Request Authenticator) operation. The Request Authenticator is known (unprotected in the Access-Request), meaning the attacker can launch an exhaustive off-line attack on the shared secret.

User-Password Based Password Attack

This vulnerability exploits the use of stream cipher to protect the User-Password attribute. The result is a vulnerability that allows an attacker to circumvent any authentication rate limits imposed by the client. The attacker attempts to authenticate given a valid username and a password (most likely incorrect). He then captures the associated Access-Request sent from the client, and determine the result of the MD5(Shared Secret + Request Authenticator) operation (in the same way as in the previous attack). The attacker can now replay modified Access-Request messages using the same Request Authenticator and MD5(Shared Secret + Request Authenticator) value. The only thing changed between each replay is the password. If the server has not implemented any throttle protection or user based rate limits, then the attacker can efficiently perform an exhaustive search for the correct user password.

Note that the attacker can only use this method to attack passwords that are 16 characters or less, as the User-Password protection mechanism uses a chaining method that includes the previous ciphertext in the state after the first 16 octets of output [Hil01].

Request Authenticator Based Attacks

For the RADIUS implementation to be secure, the Request Authenticator must be both unique and non-predictable. The RADIUS protocol specification does not accentuate the importance of how this value is generated. There could, therefore, be implementations that use poor Pseudo-Random Number Generators (PRNG) to generate the Request Authenticator. If the PRNG produces predictable numbers or repeats values (have a short cycle), then this reduces the level of protection.

5.3.2 Proprietary security solution

Aidon provides a proprietary security solution to encrypt application layer data on the RF NAN and WAN. They have not made the details of this solution public, which is a tactic known as "security through obscurity". The expression means that the security implementation may have vulnerabilities, but if the flaws are not known, that is assumed to be sufficient to prevent a successful attack. There are different arguments whether or not the security solution to a system should be secret. Some argue that by keeping the inner workings a secret, it makes the system less vulnerable to attacks. Others argue that keeping the inner workings a secret may improve security in the short term, but in the long run only systems that have been published and analyzed should be trusted. The latter argument relates to Kerckhoffs's principle, which states that *a cryptosystem should be secure even if everything about the system, except the key, is public knowledge* [Ker83]. A published and well-analyzed security solution only hinges on the secrecy of cryptographic keys. The quality of a proprietary solution, not published or analyzed, may rely on the secrecy of both the solution and the secret of cryptographic keys. If details about the cryptographic algorithms or inner workings are leaked, reverse engineered, or in some way known, then this will weaken the security. There are known examples where this has happened, e.g., the software obfuscation technique used on DVDs where the encryption used to protect the content of the DVD was broken [Sch99].

5.3.3 Mobile communication

The smart meters are intended to use mobile communication with the HES. As discussed in Chapter 2, there are known vulnerabilities in 2G, 3G, and 4G technologies. Most vulnerable is 2G(General Packet Radio Service (GPRS)), where the lack of mutual authentication makes it easy for an attacker to perform a Man-in-the-middle (MITM) attack. An attacker can mount a false base station in proximity to households

with a smart meter, and pretend to be the serving network. He can further remove a layer of security to the traffic by disabling encrypted traffic (A5/0 flag) or using an algorithm which is broken (A5/1 and A5/2). Removing a security layer will not break the confidentiality of the user data because encryption is applied at the application layer. Another option is to drop the traffic, which breaks the meters' availability to the Advanced Metering Infrastructure (AMI). It is not possible to break the integrity of messages sent between the meters and to the HES when Message Authentication Code (MAC) is used. However, Aidon uses CRC16-CCITT integrity protection for some of the messages. CRC16-CCITT does not protect against unauthorized modifications of messages which could be a potential vulnerability.

A MITM attack is possible on 3G (Universal Mobile Telecommunications System (UMTS)) by exploiting the GPRS and UMTS interoperability. Exploiting the interoperability opens up for the same vulnerabilities as for GPRS.

4G (Long-Term Evolution (LTE)) is vulnerable to IMSI catcher attacks, where an attacker can acquire subscription identities (International mobile subscriber identities (IMSI)) within an area or location in seconds, and deny access for subscribers to the mobile network. Denying the master meter access to the serving network breaks the availability to the meter and associated slaves.

To sum up, 2G and 3G are vulnerable to MITM attacks. However, Aidon have implemented mitigating strategies to reduce the consequence of such attacks. It is hard to inject or modify data because a MAC is used to maintain integrity. Furthermore, data is encrypted at the application layer. The attacker would require knowledge of the cryptographic keys to break integrity and confidentiality. This leaves the communication between the master meter and HES susceptible to Denial of Service (DoS) attacks for 2G, 3G, and 4G. A successful DoS attack could affect all the slave meters of the master.

5.4 Consequences of attacks

Based on the results of our testing, we will discuss the potential consequences of the attacks on customers and DSOs. We will mainly focus on the financial aspect. Consequences for file upload and shell access are not included since we could not confirm if these attacks were successful. Furthermore, we discuss the motivation of exploiting the associated technical risks.

5.4.1 Exposure of data from the HAN interface

Unauthorized exposure of data from the HAN interface can have consequences for both the customer and DSO. We will attempt to cover some of the consequences for

both parties.

Consequences for customers

The smart meters send detailed information about how much electricity is being used in a household. More frequent reports give a more granular picture of the power consumption. If an attacker can obtain this information, then he could gain information about the behavioral patterns of the occupants in a house. Such information can indicate when members of a house are absent or asleep [JJK⁺14]. The attacker could use this information to plan and conduct a burglary. He could also sell it, use it for marketing, or other unintended uses.

Consequences for DSOs

The consequences of leaked customer data for the DSOs are greatly affected by the data protection laws. These are the Personal Data Act (PDA) and General Data Protection Regulation (GDPR). GDPR will be incorporated into existing legal framework relating to the processing of personal data within 2018. The consequences can be divided into three groups of financial loss: operating loss, administrative fines, and liabilities [Fos17]. We will mention some of the losses for each group.

Operating loss Operating loss are losses related to the operations of the company. Some of the losses are:

- Notification loss: If customer data is leaked, the company is obliged to notify the affected persons (GDPR art. 34). Sending out notifications to customers requires resources from the DSO, especially if many customers are affected.
- Reputation loss: Leakage of customers data may reduce their trust in the company. The reputation of the company is negatively affected which may have a negative impact. However, customers can not change DSO because the DSOs have a monopoly in their operating area.
- Recovering from an attack: If an attacker successfully compromises a system or parts of a system, then security specialists are often hired to investigate or help recover from the attack. Such specialists are expensive.

Administrative fines If the DSO is not compliant with General Data Protection Law (GDPR), then the Norwegian Data Protection Authority can impose huge fines. For the most severe cases, the fines can amount to 4% of the worldwide annual revenue of the prior fiscal year. For less severe cases it may amount to a maximum of 2%. GDPR art. 83 lists 15 evaluation criteria which determine the fine. Some of these criteria are:

- Type of data breach.
- Severity of the data breach.
- Duration of the data breach.
- Any action taken by the controller or processor to mitigate the damage suffered by data subjects.
- The intentional or negligent character of the infringement.
- The degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them under Articles 25 and 32.

Liabilities The third group of consequences is liabilities. The liability can affect the company, but also executive personnel in the company. We will not look at what cases affect the two of them. It is sufficient to know that if a person suffers a loss as a result of the company not being compliant with GDPR, then that person may claim compensation for the loss.

5.4.2 Exposure of data from a MITM attack

Leaked consumption data from a MITM attack between the master meter and HES has the same impact as described in subsection 5.4.1. However, a successful MITM attack could potentially expose the consumption data from many slave meters. The consequence for an affected customer would be the same. However, the cost for the DSO would increase. More customers are affected potentially causing increased operating loss, more administrative fines, and more liabilities.

5.4.3 Denial of Service from a MITM attack

A MITM attack to perform DoS is possible. However, the consequence of such an attack is limited. The DoS attack only affects the communication over the AMI. A customer will still have access to electrical power but lose the ability to report power consumption automatically. For the DSOs, DoS attacks on the AMI will cause operating losses because they have to remedy the issue and rely on manual billing of affected customers. Both activities are time-consuming and possibly expensive. Aidon recommends somewhere between 20 and 500 slaves per master, which limits the affected customers.

5.4.4 Motivation for exploiting technical risks

The skills required to exploit the technical risks successfully suggest that the type of attacker would be hackers or organized attackers. There was not found any public

information online on how to exploit the HAN interface at the time of writing this thesis. The lack of online resources to exploit the HAN interface reduces the number of amateur hackers. Furthermore, we consider a MITM attack (over ethernet or mobile communication) to require professional knowledge of cybersecurity.

Obtaining consumption data from users is economically motivated since it could be used to perform a burglary. The attacker could also sell it, use it for marketing, or other unintended uses. DoS attacks, on the other hand, could be both economical and political motivated. The economic motivations are sabotage or blackmailing. Political motivations are a bit harder to define since it varies significantly between different groups of people. However, some of them could be the disruption or control of targets, protests, and retaliatory attacks. The size of an attack depends on how many slave nodes are connected to a master and would affect the motivation for the attacker.

5.5 Future security

It remains to see what security solution the government lands on for the HAN interface. Several suggestions have been made by leading producers of AMI solutions, including Aidon. It is important that the final solution safeguard the interest of consumers and producers. This requires increased competency and awareness of cybersecurity among politicians. The smart metering plan to be deployed in the UK was close to making a huge encryption error, which could have left the UK's 53 million smart meters wide open to hacking [Bur16]. It was planned to use a single encryption key to encrypt all traffic from the meters. Fortunately, the Government Communications Headquarters (GCHQ) intervened in the plans before realization. The installation of smart meters in Norway without a finalized security solution for the HAN interface, may indicate that security is not a high enough priority among politicians. More public services will be digitized in the future [Reg16]. This requires cybersecurity to permeate all projects, not only digitization of the electric grid.

Chapter 6

Conclusion

The goal of this thesis was to assess the security of some communication interfaces on the smart meter. The research question is *Are there security vulnerabilities in the communication interfaces on smart meters?* The research question is broad, and testing for all vulnerabilities would take too much time. Therefore, we used some time to scope down what potential vulnerabilities we wanted to test. The work consisted of identifying relevant interfaces, obtaining documentation and information about potential vulnerabilities for those interfaces, and testing them. We identified two potential security vulnerabilities. One in the Home Area Network (HAN) interface, and one in the mobile communication between the meter and Head End System (HES). We were only able to confirm the vulnerability in the HAN interface.

We identified six interfaces on the smart meter which are Ethernet, External antenna connector (local Aidon RF2), External antenna connector (uplink 2G/3G/4G), HAN interface, RS232 interface, and the status input connection. Ethernet, 2G, 3G, and 4G can be used to communicate with the HES. RF signal is used for communication in the RF NAN. The HAN and RS232 interface is used for communication between the meter and third-party equipment. The status input connection interface is used for local maintenance personnel to communicate with the meter. A threat model was used to identify threats to the Advanced Metering Infrastructure (AMI). 32 threats were found, all related to the six interfaces.

General Packet Radio Service (GPRS) lacks mutual authentication between the Mobile Station (MS) and the serving network. The lack of mutual authentication makes the technology susceptible to Man-in-the-middle (MITM) attacks. Universal Mobile Telecommunications System (UMTS) can be insecure because of its GPRS interoperability, potentially making it prone to the same vulnerabilities as for GPRS. Long-Term Evolution (LTE) has some vulnerabilities as well, e.g., IMSI-catcher attacks.

An analysis of the existing security implementation for Aidon meters suggested

that they used a comprehensive security solution. Aidon uses one or more layers of security for all communication. In addition to security in the infrastructure (e.g., mobile communication technology), they provide an extra layer of encryption (based on AES-128 CBC) which is applied at the application layer. Aidon uses a key hierarchy to handle encryption and authentication of devices. The cryptographic keys are unique for each smart meter. Different keys are used between meters in the RF NAN and between master meters and the HES. Key management is done using Aidon's own key management solution. We do not have any details of the solution, other than the different entities involved and their function. The only interface where data is not encrypted is the HAN interface. This data is not encrypted because The Norwegian Water Resources and Energy Directorate (NVE) has not decided about the security of this interface yet. The integrity of messages is maintained using HMAC-SHA1 or CRC16-CCITT. HMAC-SHA1 protects both the authenticity and integrity of a message, while CRC16-CCITT only protects against random errors. Messages that are integrity protected using CRC16-CCITT are therefore vulnerable to unauthorized modifications.

The results from testing the HAN interface confirms that consumption data is sent unencrypted from the interface. We attempted to upload data to the meter over the HAN interface. The transmission was confirmed to be successful by the software used for uploading the data. However, the link layer protocol for the HAN interface is unidirectional by default. It should therefore not be possible to push data to the meter. We were not able to confirm whether the data was received or just dropped. It would be possible to upload malicious content to the meter if the data was successfully received. We were not able to obtain shell access on the meter using scripting over the HAN and RS232 interface.

The MITM attempt between the meter and HES using the Ethernet interface suggested that the meter tries to authenticate with the serving network. Aidon confirmed that the meter attempts to authenticate using the Remote Authentication Dial-In User Service (RADIUS) authentication protocol [Ped18]. RADIUS has some known vulnerabilities caused by the use of the MD5 algorithm to protect the User-Password attribute. Some of these vulnerabilities may be present if Aidon have implemented RADIUS using the PAP authentication scheme, but our research has not confirmed this.

For future work, it would be interesting see if Joint Test Action Group (JTAG) testing on the circuit board of the smart meter could enable direct access to the Microcontroller Unit (MCU) flash memory of the meter. This is where encryption keys are stored. Compromising the keys would break the confidentiality and integrity of data sent from the master meter, potentially affecting data for many customers.



A.1 shell_script.txt

```
# Generic UNIX login script.
# Can be used to automatically login to almost every UNIX
  box.
#
  # Some variables.
  set a 0
  set b a
  print Trying to Login..
  # Skip initial 'send ""', it seems to matter sometimes..
  goto skip
loop1:
  # Send loginname not more than three times.
  send ""
  inc a
skip:
  if a > 3 goto failed1
  expect {
    "ogin:"
    "assword:"      send ""
    "NO_CARRIER"   exit
    timeout 60      goto loop1
  }
loop2:
  send "${LOGIN}"

  # Send password not more than three times.
  inc b
  if b > 3 goto failed1
```

```

expect {
    "assword:"
    "ogin:"          goto loop2
    timeout 60      goto loop2
}
send "$(PASS)"
# If we don't get "incorrect" within 3 seconds, it's probably OK.
# If they ask for a terminal, we are logged in. Tell them we're
# using vt100.
# If we get the bash prompt, send them the screen geometry.
expect {
    "TERM="          goto wantterm
    "incorrect"      goto loop1
    "bash$"          goto screengeom
    timeout 3        break
    "asswd"          break
}
exit
wantterm:
send "vt100"
exit
screengeom:
send "stty rows $(TERMLIN) columns 80"
# If you use a display mode with some other width than 80 columns,
# you may want to use the following format.
#send "stty rows $(TERMLIN) columns $(COLUMNS)"
exit
failed1:
print \nLogin Failed (wrong password?)
exit

```

References

- [3GP17a] 3GPP. 3G Security; Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification. <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2391>, 2017. (Date last accessed 06-06-2018).
- [3GP17b] 3GPP. 3GPP: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 14). <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2262>, 2017. (Date last accessed 06-06-2018).
- [3GP18] 3GPP. GPRS and EDGE. <http://www.3gpp.org/technologies/keywords-acronyms/102-gprs-edge>, 2018. (Date last accessed 06-06-2018).
- [Acc17] NTNU Accel. Hark technologies. <https://ntnuaccel.no/portfolio/hark-technologies/>, 2017. (Date last accessed 06-06-2018).
- [Aid15] Aidon. Local HAN Interface, Product Description. Confidential, 2015.
- [Aid17a] Aidon. Aidon RF2 System Modules, 2017. (Document received from Aidon).
- [Aid17b] Aidon. Our Solutions - Smart Energy Service Devices. <https://www.aidon.com/our-solutions/#devices>, 2017. (Date last accessed 06-06-2018).
- [And11] Kim J Andreasson. *Cybersecurity: public sector threats and responses*. CRC Press, 2011.
- [AS17] SINTEF Energi AS. Evaluering av NVEs veileder til sikkerhet i AMS. http://publikasjoner.nve.no/rapport/2017/rapport2017_44.pdf, 2017. (Date last accessed 06-06-2018).
- [AW11] J. Andress and S. Winterfeld. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Elsevier, 2011.
- [BBK03] Elad Barkan, Eli Biham, and Nathan Keller. Instant ciphertext-only cryptanalysis of GSM encrypted communication. In *Annual International Cryptology Conference*, pages 600–616. Springer, 2003.

- [Bie17] Lammert Bies. On-line CRC calculation and free library. <https://www.lammertbies.nl/comm/info/crc-calculation.html>, 2017. (Date last accessed 30-05-2018).
- [BSW00] Alex Biryukov, Adi Shamir, and David Wagner. Real Time Cryptanalysis of A5/1 on a PC. In *International Workshop on Fast Software Encryption*, pages 1–18. Springer, 2000.
- [Bur16] Graeme Burton. GCHQ intervenes to prevent catastrophically insecure UK smart meter plan. <https://www.theinquirer.net/inquirer/news/2451793/gchq-intervenes-to-prevent-catastrophically-insecure-uk-smart-meter-plan>, 2016. (Date last accessed 06-06-2018).
- [CJ18] Rory Cellan-Jones. Facebook scandal 'hit 87 million users'. <http://www.bbc.com/news/technology-43649018>, 2018. (Date last accessed 30-05-2018).
- [CPS+98] Fred Cohen, Cynthia Phillips, Laura Painton Swiler, Timothy Gaylor, Patricia Leary, Fran Rupley, and Richard Isler. A cause and effect model of attacks on information systems: Some analysis based on that model, and the application of that model for cyberwarfare in cid. *Computers & Security*, 17(3):211–221, 1998.
- [CR00] A. Rubens W. Simpson C. Rigney, S. Willens. Remote Authentication Dial In User Service (RADIUS). RFC 2865, RFC Editor, June 2000.
- [Dev17] DeviceHive. IoT Privacy and Security Challenges for Smart Home Environments. <https://hackernoon.com/iot-privacy-and-security-challenges-for-smart-home-environments-c91eb581af13>, 2017. (Date last accessed 06-06-2018).
- [Dev18] Analog Devices. ADE7880 - Polyphase Multifunction Energy Metering IC with Harmonic Monitoring. <http://www.analog.com/en/products/analog-to-digital-converters/integrated-special-purpose-converters/energy-metering-ics/ade7880.html>, 2018. (Date last accessed 06-06-2018).
- [Dic18] Oxford English Dictionary. <https://en.oxforddictionaries.com/definition/terrorism>, 2018. (Date last accessed 04-06-2018).
- [EJ03] Patrik Ekdahl and Thomas Johansson. Another attack on A5/1. *IEEE Transactions on Information Theory*, 49(1):284–289, 2003.
- [Eur17] European Committee for Electrotechnical Standardization. EN 62056-7-5. <http://www.standard.no/nettbutikk/sokeresultat/?search=EN+62056-7-5&subscr=1>, 2017. (Date last accessed 06-06-2018).
- [Far10] H. Farhangi. The path of the smart grid. *IEEE Power and Energy Magazine*, 8(1):18–28, January 2010.
- [fES15] European Committee for Electrotechnical Standardization. En 62056. https://ec.europa.eu/eip/ageing/standards/ict-and-communication/data/en-62056_en, 2015. (Date last accessed 06-06-2018).

- [Fos17] Kristian Foss. EUs nye personvernregler: Dette er konsekvensene av å sove i timen. <https://www.digi.no/artikler/kommentar-eus-nye-personvernregler-dette-er-konsekvensene-av-a-sove-i-timen/378590>, 2017. (Date last accessed 06-06-2018).
- [Fun17] Brian Fung. Tesla’s enormous battery in Australia, just weeks old, is already responding to outages in ‘record’ time. <https://tinyurl.com/y76mqwnv>, 2017. (Date last accessed 06-06-2018).
- [Gro01] HW Group. PortStore5: Full RS-232 serial port to Ethernet with logging. https://www.hw-group.com/products/PortStore5/PortStore5_serial-port-logger_en.html, 2001. (Date last accessed 04-06-2018).
- [GSM⁺11] Robin Gandhi, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu, and Phillip Laplante. Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine*, 30(1):28–38, 2011.
- [Har16] Michael Hardy. Energy: A networked system on which everything else relies. <https://www.federaltimes.com/smr/critical-infrastructure/2016/07/11/energy-a-networked-system-on-which-everything-else-relies/>, 2016. (Date last accessed 31-10-2017).
- [Her16] Alex Hern. Smart electricity meters can be dangerously insecure, warns expert. <https://www.theguardian.com/technology/2016/dec/29/smart-electricity-meters-dangerously-insecure-hackers>, 2016. (Date last accessed 06-06-2018).
- [Hil01] Joshua Hill. An Analysis of the RADIUS Authentication Protocol. <http://www.untruth.org/~josh/security/radius/radius-auth.html>, 2001. (Date last accessed 06-06-2018).
- [Hof17] Knut Hofstad. Energi i Norge. https://snl.no/energi_i_Norge, 2017. (Date last accessed 06-06-2018).
- [Hou09] White House. Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure. *Washington, DC: The White House Retrieved September, 3:2009*, 2009.
- [Huo07] Lasse Huovinen. Authentication and security in gprs environment: An overview. *Department of Computer Science and Engineering, Helsinki University of Technology*, 2007.
- [Ins08] Software Engineering Institute. Vulnerability Note VU836068. <https://www.kb.cert.org/vuls/id/836068>, 2008. (Date last accessed 01-06-2018).
- [Ins17] Infosec Institute. CIA Triad. <http://resources.infosecinstitute.com/cia-triad/#gref>, 2017. (Date last accessed 06-06-2018).
- [Ins18] SANS Institute. Netcat cheat sheet. https://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf, 2018. (Date last accessed 06-06-2018).

- [Inv18] Investopedia. Business asset. <https://www.investopedia.com/terms/b/business-asset.asp>, 2018. (Date last accessed 05-06-2018).
- [JJK⁺14] Ming Jin, Ruoxi Jia, Zhaoyi Kang, Ioannis C Konstantakopoulos, and Costas J Spanos. Presencesense: Zero-training algorithm for individual presence detection based on power monitoring. In *Proceedings of the 1st ACM Conference on Embedded Systems for Energy-Efficient Buildings*, pages 1–10. ACM, 2014.
- [Joh15] Finn Erhard Johannessen. Elektrifiseringen av hjemmet. <https://www.norgeshistorie.no/forste-verdenskrig-og-mellomkrigstiden/artikler/1621-elektrifiseringen-av-hjemmet.html>, 2015. (Date last accessed 04-06-2018).
- [JTK13] Martin Gilje Jaatun, Inger Anne Tøndel, and Geir M. Køien. Gprs security for smart meters. In Alfredo Cuzzocrea, Christian Kittl, Dimitris E. Simos, Edgar Weippl, and Lida Xu, editors, *Availability, Reliability, and Security in Information Systems and HCI*, pages 195–207, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.
- [Kel17] Keld Norman. How to make a simple \$7 IMSI Catcher. https://www.youtube.com/watch?v=UjwgNd_as30, 2017. (Date last accessed 06-06-2018).
- [Ker83] A Kerckhoffs. Military cryptography. *French Journal of Military Science*, 1883.
- [Kjø11] Gerd H. Kjølle. https://www.sintef.no/globalassets/project/vulnerability-and-security/publications/presentations/foredrag_gkj_fremtidens-kraftnett_sikkerhetsdagene-2011.pdf, 2011. (Date last accessed 16-10-2017).
- [Kom15] Norsk Elektroteknisk Komite. AMS + HAN. <https://www.nek.no/wp-content/uploads/2017/01/AMS-HAN-utredning-NEK-20150122.pdf>, 2015. (Date last accessed 06-06-2018).
- [Kov17] Eduard Kovacs. Smart Meters Pose Security Risks to Consumers, Utilities: Researcher. <https://www.securityweek.com/smart-meters-pose-security-risks-consumers-utilities-researcher>, 2017. (Date last accessed 06-06-2018).
- [Lyo18] Gordon Lyon. Nmap. <https://nmap.org/>, 2018. (Date last accessed 06-06-2018).
- [Mar16] Martin Eian. Lecture notes in Wireless Network Security (TTM4137), 2016. Norwegian University of Science and Technology.
- [McI18] Spencer McIntyre. Termineter. <https://github.com/securestate/termineter>, 2018. (Date last accessed 06-06-2018).
- [McN15] Simon McNair. isc-dhcp-server. <https://help.ubuntu.com/community/isc-dhcp-server>, 2015. (Date last accessed 06-06-2018).

- [MO17] Stig F. Mjølsnes and Ruxandra F. Olimid. Easy 4G/LTE IMSI Catchers for Non-Programmers. In Jacek Rak, John Bay, Igor Kottenko, Leonard Popyack, Victor Skormin, and Krzysztof Szczypiorski, editors, *Computer Network Security*, pages 235–246, Cham, 2017. Springer International Publishing.
- [MW04] Ulrike Meyer and Susanne Wetzel. A man-in-the-middle attack on umts. In *Proceedings of the 3rd ACM workshop on Wireless security*, pages 90–97. ACM, 2004.
- [53] Norwegian Electrotechnical Committee (NEK). Nek 399. http://www.standard.no/fagomrader/elektrofag/elektro/nek-399_2014/, 2018. (Date last accessed 06-06-2018).
- [Nor17a] Energi Norge. The electricity grid. <https://energifaktanorge.no/en/norsk-energiforsyning/kraftnett/>, 2017. (Date last accessed 06-06-2018).
- [Nor17b] Energi Norge. Kraftsystemet. <https://www.energinorge.no/fagomrader/stromnett/kraftsystemet>, 2017. (Date last accessed 06-06-2018).
- [NVE17] NVE. AMS. <https://www.nve.no/reguleringsmyndigheten-for-energi-rme-marked-og-monopol/sluttbrukermarkedet/ams/>, 2017. (Date last accessed 06-06-2018).
- [ob01] Justis og beredskapsdepartementet. Lov om behandling av personopplysninger (personopplysningsloven). <https://lovdata.no/dokument/NL/lov/2000-04-14-31>, 2001. (Date last accessed 04-06-2018).
- [oe11] Olje og energidepartementet. Kapittel 4. Avanserte måle- og styringssystem. https://lovdata.no/dokument/SF/forskrift/1999-03-11-301/KAPITTEL_4#KAPITTEL_4, 2011. (Date last accessed 30-05-2018).
- [oe12] Olje og energidepartementet. Meld. St. 14 (2011–2012): Vi bygger Norge – om utbygging av strømmettet. <https://www.regjeringen.no/no/dokumenter/meld-st-14-20112012/id673807/>, 2012. (Date last accessed 31-10-2017).
- [oe14] Olje og energidepartementet. Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften). <https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157>, 2014. (Date last accessed 06-06-2018).
- [oe16] Olje og energidepartementet. Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven): § 4-6 and § 4-7. https://lovdata.no/dokument/NL/lov/1990-06-29-50/#KAPITTEL_4, 2016. (Date last accessed 03-06-2018).
- [oe17] Olje og energidepartementet. Strømmettet. <https://energifaktanorge.no/norsk-energiforsyning/kraftnett/>, 2017. (Date last accessed 06-06-2018).
- [oe18] Olje og energidepartementet. The Power Market. <https://energifaktanorge.no/en/norsk-energiforsyning/kraftmarkedet>, 2018. (Date last accessed 06-06-2018).

- [Oli17] Olimid, Ruxandra F and Mjøl̄snes, Stig F. On Low-Cost Privacy Exposure Attacks in LTE Mobile Communication, 2017. Romanian Academy, Publishing House of the Romanian Academy.
- [OWA16] OWASP. The OWASP Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology, 2016. (Date last accessed 06-06-2018).
- [OWA17] OWASP. Cryptographic storage cheat sheet. https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet, 2017. (Date last accessed 06-06-2018).
- [PDF18] Datasheets PDF. (pdf) d78f0485 datasheet download. <http://www.datasheetspdf.com/datasheet/D78F0485.html>, 2018. (Date last accessed 06-06-2018).
- [Ped18] Rolf Pedersen. Private Communication, 2018. Business Development Manager in Aidon.
- [Per12] Sally Percy. Q&a. what motivates cyber-attackers? <http://www.timreview.ca/article/838>, 2012. (Date last accessed 06-06-2018).
- [Reg15] Regjeringen. Meld. st. 25 (2015–2016). <https://www.regjeringen.no/no/dokumenter/meld.-st.-25-20152016/id2482952/sec1>, 2015. (Date last accessed 06-06-2018).
- [Reg16] Regjeringen. Digital agenda for Norge: IKT for en enklere hverdag. <https://www.regjeringen.no/no/aktuelt/digital-agenda-for-norge--ikt-for-en-enklere-hverdag/id2484184/>, 2016. (Date last accessed 06-06-2018).
- [RG91] Deborah Russell and GT Gangemi. *Computer security basics*. O’Reilly Media, Inc., 1991.
- [RGSFCMSG18] A. M. Rea-Guaman, T. San Feliu, J. A. Calvo-Manzano, and I. D. Sanchez-Garcia. Systematic review: Cybersecurity risk taxonomy. In Jezreel Mejia, Mirna Mu˜noz, ˆAlvaro Rocha, Yadira Qui˜nez, and Jose Calvo-Manzano, editors, *Trends and Applications in Software Engineering*, pages 137–146, Cham, 2018. Springer International Publishing.
- [Rob15] Francesco Robino. Scripting over serial link with minicom. <https://sites.google.com/site/francescosblogg/blog/scriptingoverseriallinkwithminicom>, 2015. (Date last accessed 06-06-2018).
- [Ros17] Knut A Rosvold. kraftselskap. <https://snl.no/kraftselskap>, 2017. (Date last accessed 30-05-2018).
- [Sch99] Bruce Schneier. DVD Encryption Broken. https://www.schneier.com/essays/archives/1999/11/dvd_encryption_broke.html, 1999. (Date last accessed 02-06-2018).
- [Sch05] Bruce Schneier. SHA-1 Broken. https://www.schneier.com/blog/archives/2005/02/sha1_broken.html, 2005. (Date last accessed 06-06-2018).

- [Sho14] A. Shostack. *Threat Modeling: Designing for Security*. Wiley, 2014.
- [SM14] Paul Willmott Shahar Markovitch. Accelerating the digitization of business processes. <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/accelerating-the-digitization-of-business-processes>, 2014. (Date last accessed 06-06-2018).
- [SS04] Frank Swiderski and Window Snyder. *Threat Modeling (Microsoft Professional)*, volume 7. Microsoft Press, 2004.
- [SSR13] Paulo Shakarian, Jana Shakarian, and Andrew Ruef. *Introduction to cyberwarfare: A multidisciplinary approach*. Newnes, 2013.
- [Sta14] Statnett. Main grid operator. <http://www.statnett.no/en/About-Statnett/What-Statnett-does/Main-grid-operator/>, 2014. (Date last accessed 06-06-2017).
- [Sta17] Statnett. Nettutviklingsplan 2017. <http://www.statnett.no/Global/Dokumenter/NUP%202017-enedelig/Nettutviklingsplan%202017.pdf>, 2017. (Date last accessed 06-06-2018).
- [Sta18] Statista. Forecast market size of the global smart home market from 2016 to 2022 (in billion U.S. dollars). <https://www.statista.com/statistics/682204/global-smart-home-market-size/>, 2018. (Date last accessed 06-06-2018).
- [Tel13] Telenor. Smart metering white paper – Best practices recommendation by Telenor Connexion, 2013.
- [TH16] M. Longva P. Hai B. Tong H. Willett T. Hagelien, I. Hessevik. Penetration testing of patched Patentsy web application. Project in the course TDT4237 at NTNU, 2016.
- [TJL13] Inger Anne Tøndel, Martin Gilje Jaatun, and Maria Bartnes Line. Threat modeling of ami. In Bernhard M. Hämmerli, Nils Kalstad Svendsen, and Javier Lopez, editors, *Critical Information Infrastructures Security*, pages 264–275, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.