Attack scenarios on AMI that Compromise Human Behaviour and Cellular Networks

Thesis submitted in partial fulfillment of the requirements for the degree of

Master in Programming and System Architecture

to the The Faculty of Mathematics and Natural Sciences, at the University of Oslo.

Namrah Azam

Reliable Systems Group

Department of Informatics, University of Oslo

Supervisors:

Christian Johansen, UiO

Janne Hagen, The Norwegian Water Resources and Energy Directorate

Jon-Martin Pettersen, PhD

Abstract

The advanced metering infrastructure (AMI) is being rapidly deployed throughout the Smart Grid. Introducing this technology into the power grid forces the energy industry to address new cyberthreats towards this critical infrastructure. A necessary first step in achieving cybersecurity in the Smart Grid is identifying the attack surface on AMI. The prominent and dominating attacks within the digital domain are social engineering and wireless network attacks. In response, the purpose of this thesis is to quantify and examine the attack surface of AMI (particularly focusing on the Norwegian deployment) in terms of leveraging mobile communication networks and the human factor in the system. We demonstrate, using attack scenarios, how social engineering and network attacks may be used as entry vectors in launching cyberattacks on AMI and exploiting its components. The examples described here demonstrate how threat agents can use these techniques against AMI. The thesis also describes the consequences of such attacks.

Acknowledgements

I want to express my deepest appreciation to my thesis supervisor Professor Christian Johansen from the University of Oslo, Department of Informatics. He has been patient with me, and I appreciate the guidance, encouragement, and helpful advice he provided me throughout my master's. I am lucky to have a supervisor who cared about my work, motivated me to finish my thesis, and promptly responded to my questions and queries.

I want to thank my external co-supervisors from Norwegian Water Resources and Energy Directorate (NVE), Ph.D. student Jon-Martin Pedersen and Dr. Janne Hagen for not only supporting and supervising me through the initial course of my masters but motivating me and helping me towards my work career. I feel very grateful to have had the opportunity to work with NVE and Jon-Martin and Janne as my co-supervisors.

My sincere gratitude goes out to professor and dean Tore Pedersen, at Norwegian Defence Intelligence School. I thank him for providing me with relevant content for my thesis; his feedbacks have improved my work.

Towards the long journey to this degree, there have been many scripts that I wasn't able to compile and many bugs I wasn't able to find on my own. I am truly thankful to my friends for helping me overcome difficult problems whenever I need it. I thank you for your companionship and for making my time at IFI enjoyable and memorable.

At last, I want to thank my sister and mother. My lovely family, I would never have been able to complete my degree without your support and love.

Thank you Lord,
for always blessing me with more than I deserve

Contents

List of Figures

List of Tables

Dedicated to my mother, my dear amma,
who never stopped giving of herself in countless ways, supporting me through everything. Her prayers, love, courage, and devotion has been the strength of my every achievement.

Chapter 1

Introduction

Digital technology is transforming industries across multiple aspects of society, influencing business perspectives, the world economy, and the human lifestyle in terms of the ways humans interact with each other and with machines.

The digital agenda is driven by the fusion of different information technology trends, such as cloud computing, machine learning, and big data. These, along with many other technologies, data, and intelligence, are at the center of digitization. Industries and businesses are located in a constantly changing world that is more volatile and complex than ever. This change has a significant impact on all segments of our society, from the massive industries to factories to household consumption and the individual's use of technology.

As part of a socio-complexed system, greater flexibility, speed, and digital skills are needed. While it is clear that digital technology is transforming most industries positively, such as simplification and automation of many tasks, many challenges still need to be addressed. These include factors such as the pace of changing customer expectations, cultural transformation, outdated regulation, identifying and accessing the right skills, and the topic of this thesis: cybersecurity in the digital domain.

The speed and extent of the digital transformation also affect critical infrastructure such as the energy sector, which this master thesis addresses. Digitization offers the opportunity to develop smart and efficient energy solutions for homes and more efficient operations in companies. Digital technologies are used to control energy production, distribute, transfer information about consumption, and monitor demand.

The ever-increasing components' exposure and connection to the Internet make critical infrastructures such as the energy sector, vulnerable to cyberthreats and unwanted events. The way every component, such as in industrial control systems, smart networks, and digital systems, is interconnected has triggered various security issues. Power grids are fast becoming digital jungles, integrating the Internet of Things (IoT) sensors, smart meters, and cloud services. This jungle is introducing new considerations for organizations concerning hackers, cybersecurity, and data protection.

The energy sector is a critical infrastructure that must be protected from possible security breaches and cyberattacks that may result in information theft, interruptions, failure, blackouts, energy theft, customer privacy breach, endangered safety of operating personnel. Potential attacks could result in fatal consequences. The worst-case scenario of a breach could lead to an outcome where nature or human life is compromised.

1.1 Motivation

This thesis addresses issues on cybersecurity in the advanced metering infrastructure (AMI) as pitfalls need to be taken into account when considering IoT technologies in the energy industry. Despite the undeniable advantages of merging information technology (IT) and operational technology (OT), smart solutions have their implications. They pose significant cybersecurity risks when connected to the world wide web. The risk of being exposed to threat agents increases as the number of devices linked to each other and the Internet grows. Security attacks on IoT are alarming in numbers. Security incidents happen because of poor security practices performed in IoT, such as security measures not being implemented correctly, if at all, systems not being patched or configured appropriate, the large number of devices and users, and the fact that IoT does not has one standard communication protocol, but a variety of communication protocols, technologies and channels.

The motivation for this thesis comes from the numerous recent cyberattacks on critical infrastructure. Many cyber threat actors are motivated to launch an attack on the power grid, ranging from economic reasons (e.g., reducing electricity bills) to pranks and terrorism (e.g., threatening people by controlling electricity and other life-critical resources). While benefiting the benign participants (consumers, utility companies), the emerging Smart Grid poses many vulnerable entries, serving as powerful tools for adversaries to exploit.

One part of the Smart Grid most affected by the IoT revolution is the advanced metering infrastructure (AMI), introducing new components connected to the Internet (e.g., smart meters). Moreover, AMI is widely spread, being present in all locations such as offices, schools, inside the now smart houses, which are even more populated with IoT than before. Hence, the importance of identifying the attack surface of AMI is essential, considering that a security breach in AMI could affect the location where the technology is rolled out, such as households, residencies, enterprises, or the whole Smart Grid.

Many IoT attacks are performed remotely and through automated mechanisms like viruses or bots (e.g., BrickerBot, RIFT botnet that infects IoT devices, or Mirai). Since IoT devices are readily available on the market, hackers (both state-sponsored actors (APT) and non-state actors) have more accessible ways of learning about these devices and tinkering with them. Due to communication networks being available everywhere, threat actors can attack devices through the network from anywhere. Thus, performing hacking is easier if one can exploit the protocols (IoT communication protocols that are short-range like Bluetooth or ZigBee, or exploiting the cellular network such as LTE-M or nb-IoT). Another attack strategy widely applied by hackers today is social engineering: the art of influencing and manipulating individuals to perform a set of actions or divulging confidential information. Recent examples Stuxnet, 3.3.4.1 and attacks on the Ukrainian Smart Grid, 3.3.4.2 demonstrate that elements of social engineering such as targeted spear-phishing or malicious software from peripheral devices, s.a. USB dongles, have been a part of the initial stages of an attack to infect the critical infrastructure.

With the addition of IoT, Smart Grid becomes an arena for both worlds of hacking: hacking the wireless networks and hacking the human brain to compromise the energy sector. Now one can imagine the outcomes when both these worlds are combined.

1.2 Method

The method used to gather information is primarily through conducting a literature review — a survey of essential articles, books, and other material on the research topic, mostly from non-technical perspectives. However, we also use some scholarly sources that have technical views as well.

We have used existing attack techniques on cellular communication networks and social engineering explained in research and literature and applied these to the threat landscape of AMI, constructing our scenarios. The scenario method is a tool that helps describe a possible set of future conditions. In our study, the scenarios describe fictional stories of attackers exploiting vulnerabilities in AMI.Exploring a range of alternative scenarios related to exploiting the human brain and cellular networks has allowed us to identify potential risks and shed light on such attacks' implications.

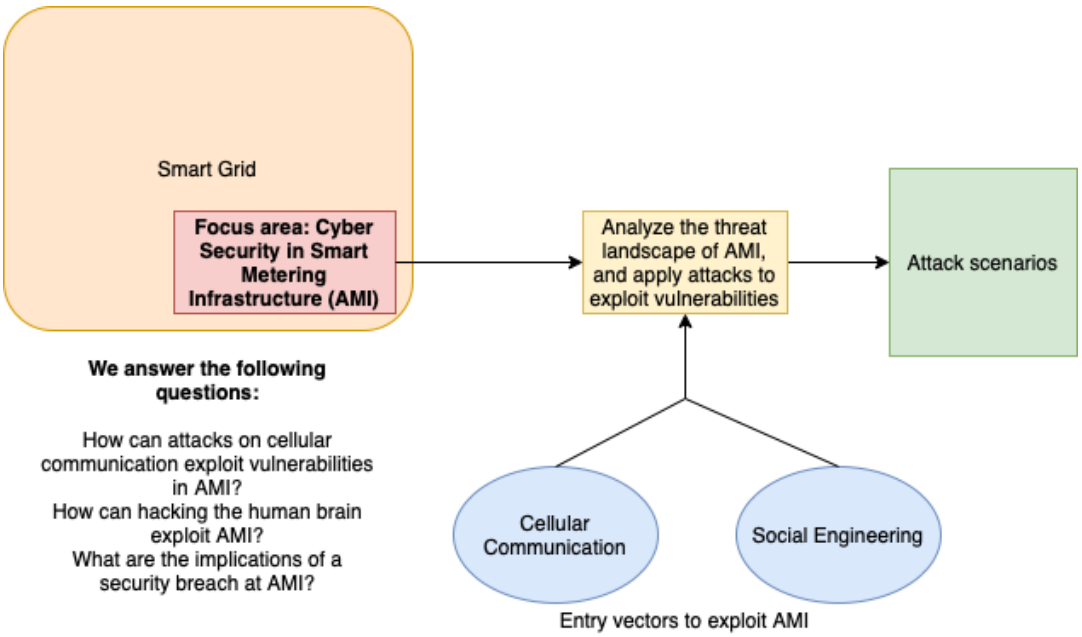

FIGURE 1.1: Method overview

1.3 Goals and research questions

The following questions will guide this thesis to its goal and will be answered through the literature review and our fictive scenarios. One main question that is being asked is *"What are the attack possibilities on the Advanced Metering Infrastructure?"*. This thesis studies two sides of this question:

A. The IoT side, or more concretely, the communication part of Advanced Metering Infrastructure, asking how can cyberattacks be performed through the existing communication means applicable to AMI?

B. The human involvement in this system, or more concretely: what possibilities are available to a determined attacker to apply known social engineering attacks to compromise AMI and its components in particular?

We start the thesis with an overview introduction to needed concepts related to Smart Grids and AMI. As such, the first part of the thesis presents aspects answering the (A) question, whereas the second part explains the (B) question by studying social engineering and presenting social engineering techniques that have been applied in the energy sector. One important aspect that we also present is the impacts of attacks on Smart Grid and AMIs. To make the presentation more realistic and to convey to the reader more concretely the implications of security attacks on smart grids, we employ the technique of story-telling, where we form stories of "what-would-happen-if" together with scenarios depicting a social engineering attack.

1.4 Thesis overview

The thesis is organized into five chapters, with an overview visually presented in Figure 1.2. Chapter 2 introduces Background information on the Smart Grid, its design, the most significant and fundamental components required to make the grid "intelligent", and why it has a vital role in the era of IoT. This chapter also gives a brief description of the subject of Advanced Metering Infrastructure and its essential components. There are many vulnerabilities linked to AMI, and the first section of chapter 3 presents the attack surface of AMI. Further sections elaborate on various attack methods that can be done through social engineering and exploiting vulnerabilities in cellular communication. Chapter 4 discusses and outlines different attack scenarios and their implications, which may be the outcome of exploiting

vulnerabilities. For the sake of clarity, instead of having a separate analysis chapter, we build the analysis into every scenario. Chapter 5 ends with a general discussion of the findings and their contribution to current research.

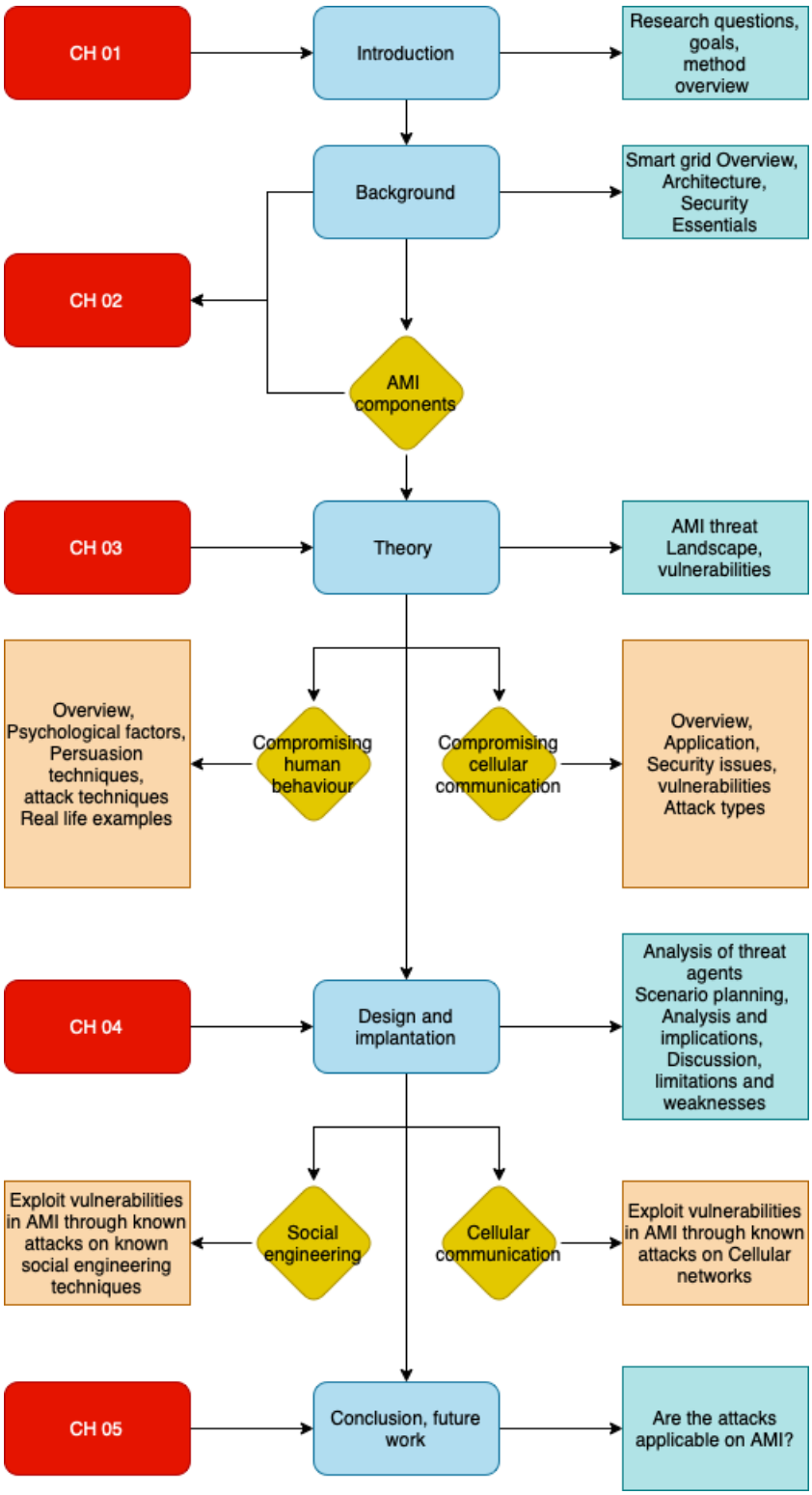

FIGURE 1.2: Thesis overiew

1.5 Contributions

This thesis demonstrates how human interaction with the system and unauthorized cellular network access may be used to attack the Advanced Metering Infrastructure. We analyze vulnerabilities in AMI and predict, evaluate, and explain the implications of attacks through a set of scenarios. This thesis makes the following contributions:

1. Presenting the threat landscape of AMI, looking into each component and identifying vulnerabilities for the respective component.
2. We show how by leveraging existing social engineering methods and cellular network attacks one could exploit AMI vulnerabilities in order to compromise the Smart Grid infrastructure. Recent attacks on critical infrastructures containing IoT have been carried our by hacker groups entering the system by compromising the human factor using social engineering techniques or compromising various wireless networks using different network attacks. We explain how a hacker may use the same attack strategies on the metering infrastructure through scenario planning.
3. State-sponsored hacking groups, cybercriminals, and hacktivists are threat agents that appear to be particularly interested in targeting the energy industry. Considering these three threat agent groups, we assess which group is most likely capable of carrying out the attacks described in the scenarios and present the implications based on this.

Chapter 2

Background

2.1 Smart Grid

Smart Grid is the collective term for the new generation power grid. The extension of Internet connectivity is used to better utilize the energy infrastructure with controls, computers, automation, new tools, and equipment. With these new technologies, the Smart Grid is intended to solve the traditional power grid problems, mainly related to uni-directional information flow and energy wastage, growing energy demand, and reliability.

In [57] Suganya, C. S. U., and Subhalakshmipriya, C. describes the Smart Grid as *"a modernized electrical grid that uses information and communication technologies to gather an act on information, such as information about the behaviors of suppliers and consumers, in an automated fashion, this to improve efficiency, reliability, economics, and sustainability of the production and distribution of electricity"* [57, p. 386]. The new electricity grid is characterized by various systems and components merged with the Internet, using a technology provided by the Internet of things(IoT)-era, which is the main idea behind the concept of Smart Grid.

IoT extends the Internet's ubiquity by integrating any object connected to the Internet for interaction through embedded systems, resulting in a highly distributed network of devices communicating with both humans and other devices (device-to-device communication). IoT technologies provide connectivity anywhere and anytime and merge different technologies to be compatible with an Internet connection.

Smart Grid's deployment has a central role in enhancing the energy infrastructure by implementing advanced IoT technologies. The components and

systems in the power grid are merged with the Internet to utilize the energy infrastructure better. These internet-connected components help provide smart devices, meaning IoT devices, such as sensors, actuators, and smart meters, for monitoring, analyzing, and controlling the Smart Grid, connectivity automation, and monitoring these devices.

The Smart Grid aims to [18]:

- minimize environmental impact
- enhance markets
- improve reliability and service
- reduce costs and improve the efficiency of electricity distribution

These factors realize the IoT-supported system that supports and improves various network functions of Smart Grid: power generation, transmission, distribution, and utilization.

Even though the Smart Grid term has experienced considerable hype in the past years, it is very apparent that the Smart Grid reflects a significant change in the way people think about the generation, delivery, and use of electric energy. As a result, the Smart Grid has come to represent an essential change in addressing the energy demand, security, and environmental challenges we face.

2.1.1 Difference between Traditional and Smart Grid

The development from the traditional electricity distribution to intelligent transport and the electricity exchange laid the Smart Grid foundation. In general, the Grid is an interconnected electricity system with characteristics such as generation, transmission, distribution, and control of electricity. Even though the traditional power grid worked quite well for about 100 years, challenges and problems occurred with time. The conventional electricity grid became hard to manage and monitor due to the increased world population and the advancement of technology. These factors resulted in an increased demand for electricity power [52].

Especially after the year 1970, the power grid continuously got updated with new technologies. The updates, upgrades in the Grid, and mass production of electronic devices resulted in a dramatic change in electrical energy consumption. Electronic devices started being used differently, compared to

previous years, when the electricity needs were simple. The electricity that previously only utilized a few devices in the home, such as radio and light bulbs, started growing with time. The growth of electronic devices led to an increased load, affected by the electricity demand and new sources of high electricity consumption in development. Due to advanced technology and the innovation of many gadgets that require a large amount of electricity, the traditional power grid was not sufficient for this use anymore [26].

The rising electricity demand was the start of the Smart Grid era. Although the basic operations in the traditional power grid and the Smart Grid are the same, the latter does differentiate in many ways. The main difference between the two grids is that the Smart Grid has a two-way data flow enabled by AMI's Advanced Metering Infrastructure. The data flow going through AMI consists of communication and electricity between the utility and its customers. The conventional Grid, on the other hand, only has one-way communication. One-way electricity distribution is that the power can be exclusively distributed using the traditional energy infrastructure from the main plant. The traditional power grids generally carry power from a few central generators to many users or customers. The Smart Grid is a growing network that integrates communications, controls, automation, new technologies, and tools to make power consumption and distribution more efficient, reliable, secure, and even greener. Smart Grid enables new technologies in the Grid, such as wind and solar energy production.

The Smart Grid can efficiently deliver power and respond to wide-ranging conditions and events by utilizing modern information technologies. Broadly stated, the Smart Grid could respond to events that occur anywhere in the Grid, such as power generation, transmission, distribution, and consumption, and adopt the corresponding strategies [52]. All of the factors mentioned above bring along significant benefits for the environment, DSOs, and consumers. Utilities can better communicate with the customers, and the customers can manage their electricity needs in their smart homes. Some of the benefits are listed below.

Smart Grid benefits [44]

- Gives the consumer's ability to access and observe their electricity usage patterns. Consumers can minimize their energy expenses by adjusting their intelligent home appliance operations to avoid peak hours and utilize renewable energy instead

- Electric utilities attempt to get customer's attention to participate in the Smart Grid system to improve services and efficiency
- It controls intelligent appliances at consumers' homes or buildings to save energy, reduce cost and increase reliability, efficiency, and transparency
- A Smart Grid is expected to be a modernization of the legacy electricity network. It provides monitoring, protecting, and optimizing automatically to the operation of the interconnected elements
- A Smart Grid senses problems and reroutes power automatically, which prevents some outages and reduces the length of those that do occur
- Smart Grid helps reduce greenhouse gas emissions by making it easier to connect renewable energy sources to the electricity grid

2.1.2 Smart Grid architecture

The Smart Grid architecture is a complex multi-layered system that allows communication, computing, and information technologies to participate and integrate with the energy infrastructure. The Smart Grid infrastructure of this advanced architecture includes intelligent energy systems and information systems, in addition to smart communication [26]. The architecture helps realize Smart Grids three main functionalities through three levels: power generation through the generation grid, electrical power transmission to utilities through the transmission grid, and electricity distribution to consumers through the distribution grid.

When the traditional Grid was introduced in the late nineteenth century, power generation was localized and built around communities [16], serving electricity through central stations to a few nearby customers. Systems once isolated and became interconnected, providing long-haul transmission, and from this developed the basic operating structure of the Grid, which is still in use today. [8] sums up the basic operating structure of a grid in the following points:

1. Large power plants generate electricity and transmit it at high-voltage levels
2. Interconnected transmission lines that transmit electricity over long distances

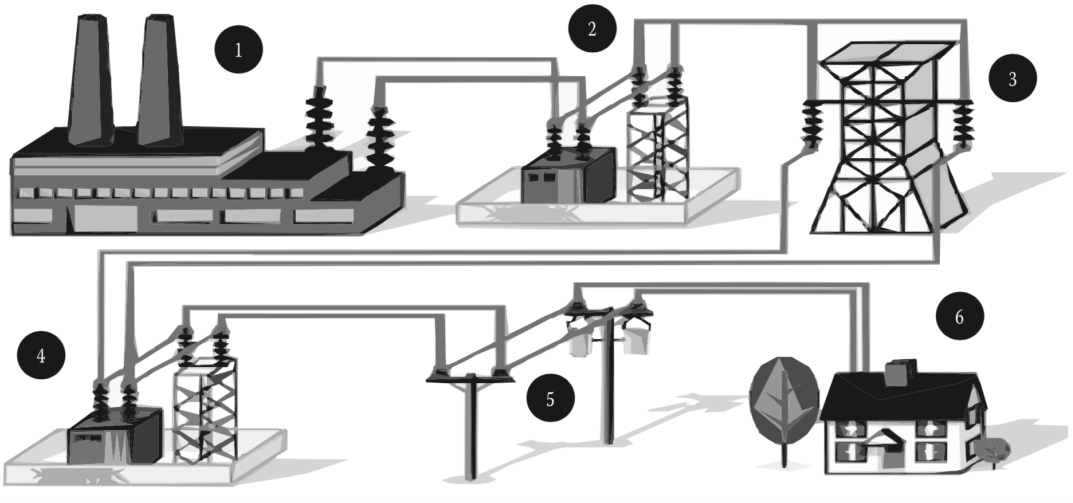

FIGURE 2.1: Electric utility interconnection overview: elements that are responsible for the fundamental operations of grid [8, p. 2]

3. Distribution substations where a transformer steps down the voltage
4. Delivery of power over relatively short distances to a network of smaller, local transformers, which step the voltage down further to levels safe and appropriate for the homes or businesses it serves

The elements that provide the basic operations of a smart grid, are illustrated in figure 2.1. *(1)* a power plant: industrial facility for the generation of electric power. *(2)* a transmission substation: transform voltage from high to low. *(3)* a transmission line(power line): used to transport electricity from place to another. *(4)* a distribution substation: deliver electric energy directly to industrial and residential consumers *(5)* a distribution line/transformer: provides the final voltage transformation in the electric power distribution system, decreases down the voltage used in the distribution lines to the level used by the customer. *(6)* an end user: consumer of the power [8]. The regulatory structures that govern the industry have evolved since the early 19th-century. The basic operating structure of the Grid has remained the same over decades, but practices to plan and operate the Grid have changed [8]. The previously simple infrastructure is now being expanded with advanced equipment, allowing increased communication between devices and facilitating remote control, self-regulation, and self-healing. Sensing technologies are embedded in the infrastructure to create a communication backbone that allows real-time data acquisition and analysis. Sensors on the line can identify abnormalities and perform minor troubleshooting and repairs without the need for human involvement. Power distribution from numerous plants

and substations is used by the Sensing Smart Grid architecture to balance the load, reduce peak time load, and reduce the amount of power outages. Such technology allows energy distribution to be monitored automatically, and personnel is not needed to handle power outages as the systems can be accessed remotely and solve complications.

For issues related to infrastructure damage, the smart Grid can immediately report to technicians at the monitoring center to begin the necessary repairs. The collected information is interpreted and delivered as reliable, robust, and meaningful to infrastructure providers to make better-informed decisions about their assets' structural health and maintenance. In a sensing environment, infrastructure can respond in real-time to users' satisfy needs. Infrastructure assets that are self-aware, control their own maintenance, resulting in condition-based maintenance, decreased downtime, and improved infrastructure operating efficiency. Better information leads to a better knowledge of infrastructure behavior. It contributes to paradigmatic changes in design and construction, as well as significant improvements in health and productivity, design and performance efficiency, a low-carbon society, and sustainable urban planning and management.

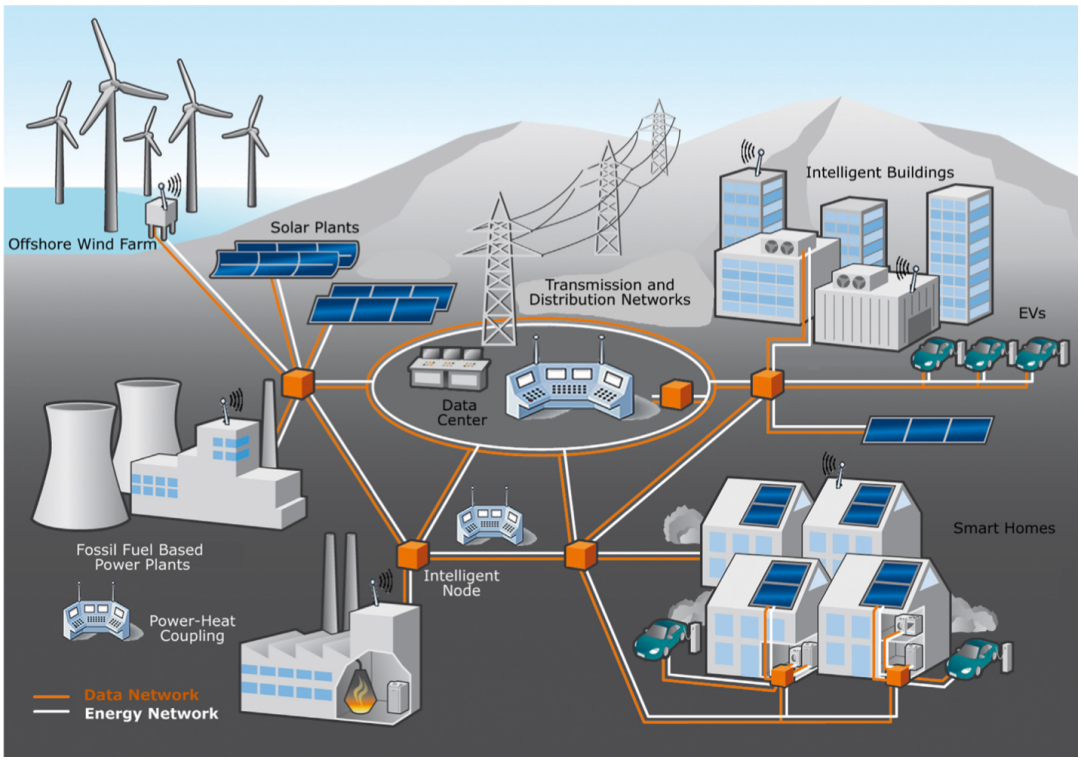

FIGURE 2.2: Smart Grid

Smart Grids do provide the same functionalities and have the same fundamental architecture, but they are designed differently; different companies,

infrastructure, and architecture can vary. Different types of architectures are related to what framework is used and which standards are applied [12][22]. This thesis does not provide an in-depth description of every layer, but a brief description of some layers is provided later in this chapter.

[22] summarizes the architecture in three main layers: the application layer, the power layer, and the communication layer. The Smart Grid architecture model (SGAM) framework, on the other hand, in 2.3, gives a more detailed view of the structure and the form of the architecture layers. The SGAM framework consists of five layers representing business objectives and processes, functions, information exchange and models, communication protocols, and components. The component layer consists of applications with advanced technologies, such as managing different services provided by the Smart Grid, related to the electrical grid Bulk Generation, Transmission, Distribution, DER, Customer Premises. It includes system actors, applications, power system equipment, network infrastructures such as wired and wireless communication connections, routers, switches, servers, and computers. The communication layer describes protocols and mechanisms for the interoperable exchange of information between components(function or service and related information objects or data models). The information layer describes the information being exchanged between functions, services, and components. The information and canonical data models represent the standard semantics for functions and services to allow an interoperable information exchange via communication means. The function layer describes functions and services, including their relationships from an architectural viewpoint. The functions are represented independently from actors and physical implementations in applications, systems, and components. The functions are derived by extracting the use case functionality, which is independent of actors. The business layer represents the business view on the information exchange related to smart grids. There are many economic and business aspects within the Smart Grid to map regulatory and economic (market) structures and policies, business models, business portfolios (product services) of market parties involved. The communication layer is relevant to this thesis.

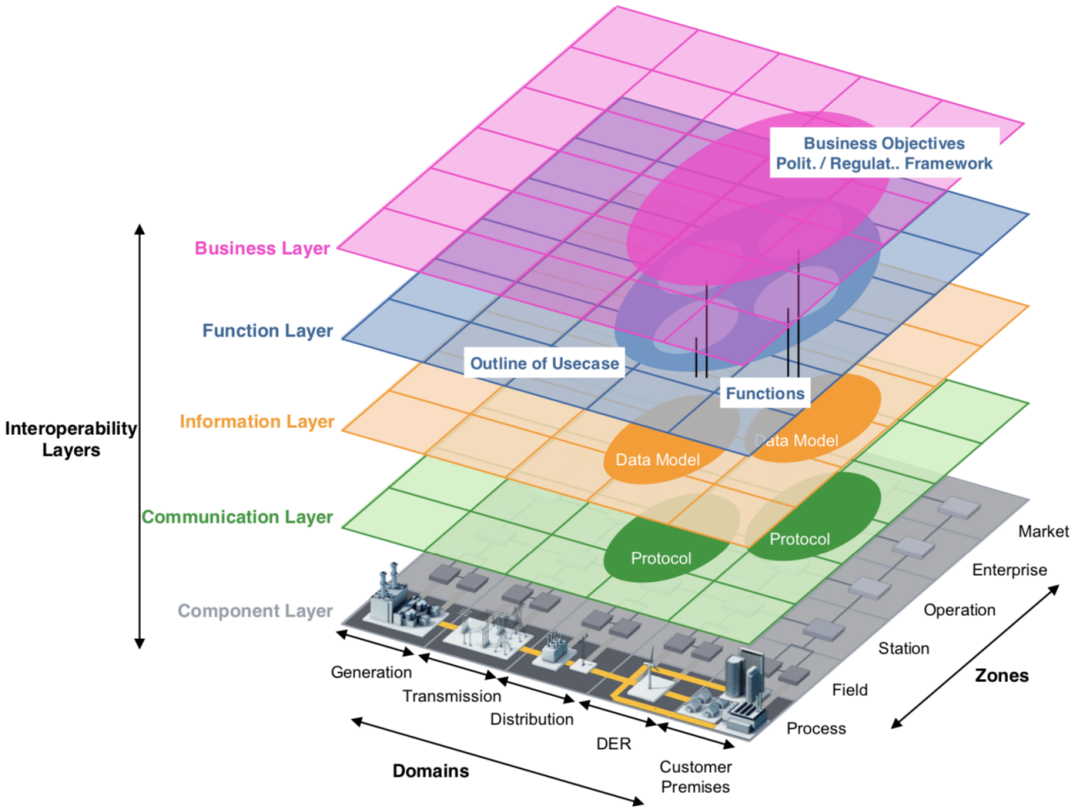

FIGURE 2.3: SGAM Framework: Architecture layers [48, p. 795]

2.1.3 Smart Grid communication architecture

The communication system is an essential part of the Smart Grid architecture, as it lays the foundation of the smart infrastructure that provides the two-way information flow. Advanced technologies and applications are integrated into the system to achieve this infrastructure. Hence, electric utilities must define and develop suitable communication standards, requirements, technologies, identify inter-operable communication protocols with standard semantic models for each domain of the smart Grid, and integrate these communication protocols for inter-domain information exchange [22][45]. Furthermore, it is essential to adapt security for the communication interfaces. This all handles the data and delivers services in a reliable, secure, and cost-effective way throughout the whole system [22].

The communication architecture of the Smart Grid includes different layers of computer networks, serving different purposes. The architecture layers are divided into categories supported by various network technologies; 2.2.4.1 provides more details on this topic. The communication infrastructure in Smart Grid must support the expected Smart Grid functionalities and meet the performance requirements. As the infrastructure connects many

electric devices and manages the complicated communication between these, it is constructed in a hierarchical architecture with interconnected individual sub-networks, each taking responsibility for their separate geographical area [62]. According to [4] the Smart Grid communication network architecture includes neighborhood area networks *(NAN)*, home area networks *(HAN)* and wide area networks *(WAN)* [1]. Figure 2.4 shows the layers of the network architecture in a Smart Grid and their connection to each other and the utility.

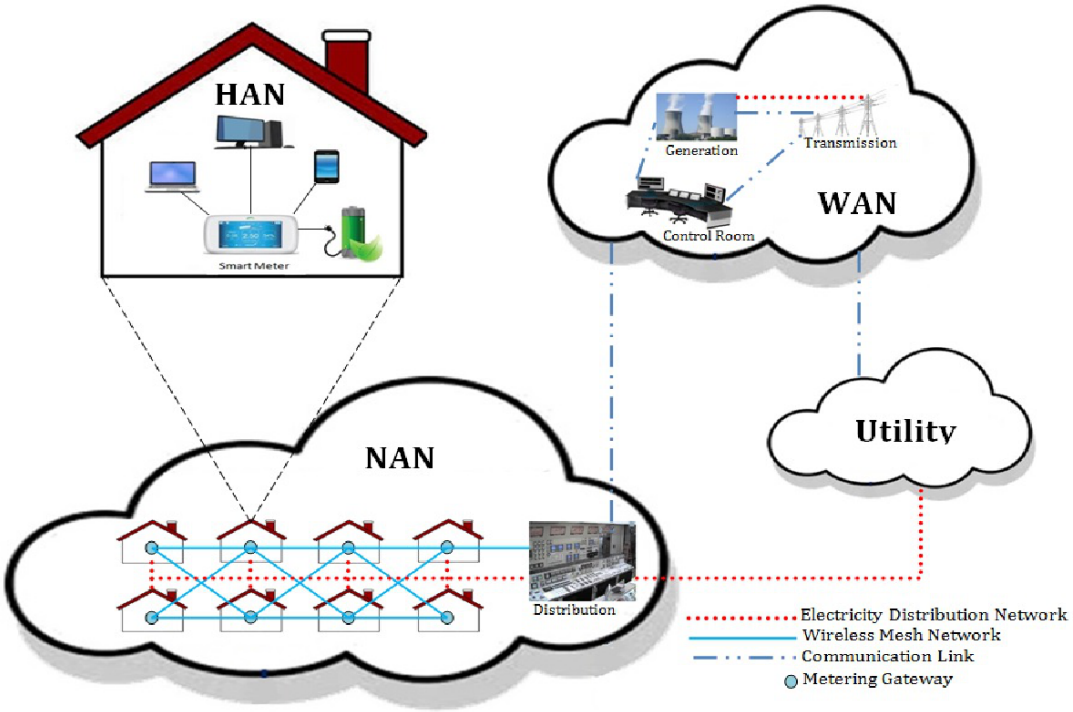

FIGURE 2.4: Smart Grid network architecture: Home Area Network *(HAN)*, Neighborhood Area Network*(NAN)*, Wide Area Network *(WAN)* [28, p. 1]

[1] Network architecture is described differently in different research papers, e.g some have included field area network (FAN) etc.

Home Area Network *(HAN)* is the first layer in the network architecture. HAN provides a connection between the smart meter and the appliances in a home, industry, or building, connecting smart meters with appliances, plug-in electrical vehicles, and distributed renewable sources, such as solar panels, wind power, and energy storage. It is a part of the network architecture that resides on the consumers' side. The smart meter connection to HAN enables consumers to be aware of their electricity usage costs, manage consumption behaviors, and control smart appliances. Other services that HAN provides are related to demand response, real-time pricing, and load control. The main requirements for communication in HAN are low cost, less power consumption, and, most importantly, secure communication. Technologies that supports HAN: ZigBee, WLAN and PLC, among others [4] [22][25][62].

Neighbourhood Area Network *(NAN)* is the second layer in the network architecture and is a part of the Advanced Metering Infrastructure as 2.5 shows in chapter 2.2. It links smart meters, distributed automation, field devices, distributed energy resources or microgrids, utility-scale storage, and concentrator. The NAN collects the metering and service data from multiple HANs and transmits this information to the data collectors that connect the NANs to the WAN [28]. The links between the smart meter and the data concentrator can be established using different communication technologies. It can use wireless technologies such as RF mesh, WiMax, and cellular networks. NAN can also be implemented by using wired networks such as PLC (Power Line communication), fiber, or cables [27] [35].

Wide Area Network *(WAN)* is the third and upper layer of the network architecture. WAN expands over a large geographical area and provides communication between the utilities and substations, including communication between distributed power generation and storage facilities [22]. It provides a two-way data communication network for communication, automation, and monitoring purposes of Smart Grid applications [4]. WAN combines two networks, a core network that provides connectivity between the utility and the substation systems and a backhaul that connects the NAN network to the core. This structure prevents power outages by providing real-time information about the power grid. Control application gives the capability of self-healing to the Smart Grid. This application helps perform a quick operation of generator tripping and provides voltage support to large power systems. The WAN connects communication between network gateways or

aggregation points, NAN, substations, distributed grid devices, and the utility data center. According to [21], cellular networks, WiMAX, and wired communications are the best communication technologies for WAN.

2.1.4 Security aspects of Smart Grid

Cyber security is a major concern for the Internet of Things domain, thus for the wide range of adoption and deployment of IoT in Smart Grid. As the IoT technologies are integrated into the Smart Grid, it becomes highly vulnerable to digital attacks. As mentioned in the introduction, the energy sector is a critical infrastructure and must be protected. If the Smart Grid or its components are affected, it could have consequences for a nation and its citizens. It emerges from many studies and researches that the Grid has many vulnerable spots. All the interconnecting devices in smart grids are susceptible to cyberattacks [52][26].

2.2 Advanced metering infrastructure and its components

Advanced metering infrastructure (AMI) is the architecture that enables Smart Grid technologies to provide operational and commercial benefits to utilities and customers. Through two-way communication between customers and utility entities, AMI gathers and analyzes data from smart meters. AMI provides the utility with valuable data like real-time voltages, currents, power flow, and power factor, as well as tracking accumulated power usage by the user for billing purposes [41].

AMI provides intelligent management of various services and applications to manage data. AMI's primary functionalities concern power measurement, assisting adaptive power pricing and demand-side management, providing self-healing abilities, and providing interfaces for other systems [14] [32]. The infrastructure has the ability to automatically and remotely measure electricity consumption, connect and disconnect services, detect tampering, identify and isolate outages, and monitor voltage.

Concisely, the main goal of this system is to provide utility companies with real-time data about their customer's power consumption and provide the customer the privilege to make informed choices about energy based on price and time of use.

As it appears, AMI is not a single technology; it is a configured infrastructure that merges many technologies that cooperate. The infrastructure is a set of subsystems that must be integrated to achieve an intelligent grid. All the components are interconnected using different communication channels and protocols, making this infrastructure a complex system of different systems extending over a large geographic area.

The primary infrastructure consists of the following main components: Smart meters, communication networks, and data management systems. All components are integrated into the system to enable two-way communication between utilities and customers, which are the service delivery endpoints [23][52][41].

Through the communication network, AMI provides a path from the smart meters to utility providers. These AMI components are located in various networks (respectively HAN, NAN, WAN) and different realms such as public and private ones. An overview of the AMI infrastructure is displayed

in figure 2.5. The figure shows in detail the network architecture and their supported network technologies in the Smart Grid, previously discussed in chapter 2.1.2 and 2.2.4.1.

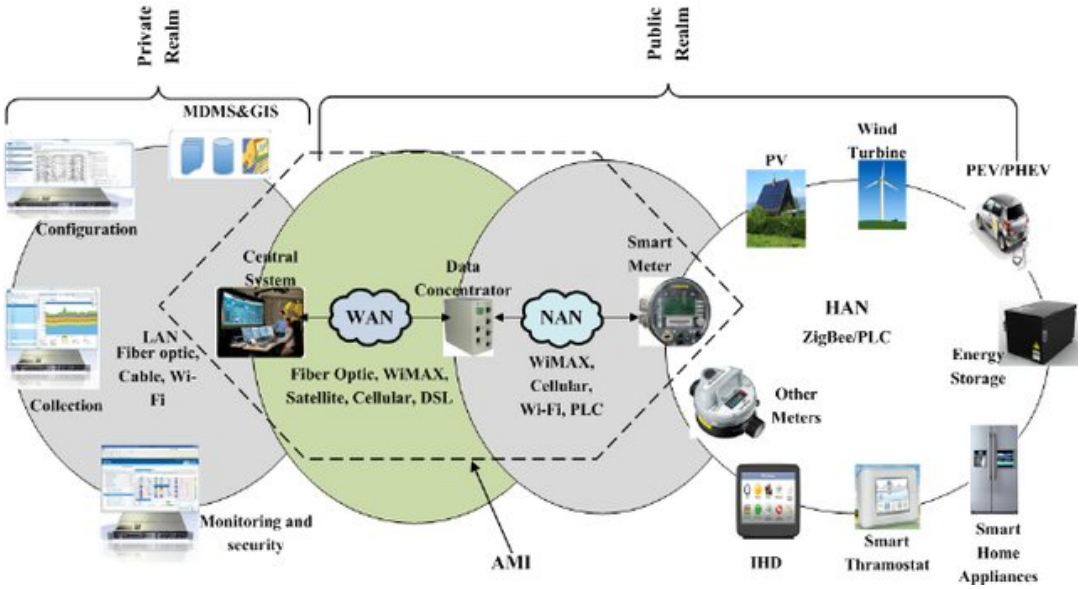

FIGURE 2.5: Advanced Meter Infrastructure overview[32, p. 42]

2.2.1 Smart meter

Smart meter is one of the key devices in AMI. The intelligent meter is responsible for monitoring and recording power consumption of home appliances in real-time, calculating energy production to meet the demand and reporting the data further to the utilities.

The electricity consumption records are sent for billing and monitoring, from the endpoint (customer) to the electricity supplier due to the two-way communication between the meter itself and the central head-end servers (utilities). The two-way communication flow is shown in figure 2.6.

[41] summarize the key factors provided by smart meters as follows:

- Time based pricing
- Providing consumption data for consumer and utility
- Net metering
- Failure and outage information
- Remote command(turn on/off) operations
- Load limiting for demand response purposes

- Power quality monitoring including: phase, voltage and current active and reactive power, power factor
- Energy theft detection
- Communication with other intelligent devices
- Improving environmental conditions by reducing emissions through efficient power consumption

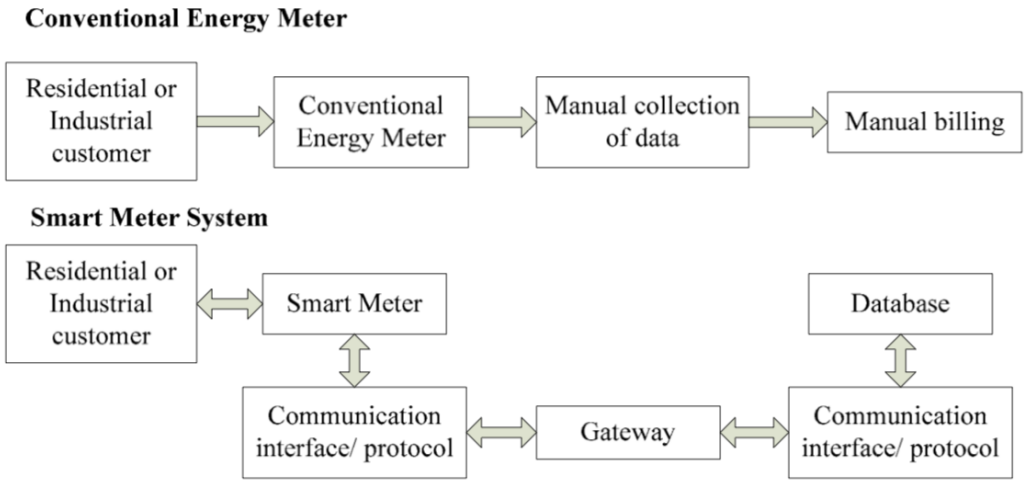

FIGURE 2.6: Metering architecture: Comparison of the analog meter and smart meter [13, p. 1]

2.2.2 Data Collectors

Data collectors, also known as concentrators, gateways or substations, are communication nodes between the smart meters and the head-end system. These nodes transfer data from the NAN-network to WAN-network [23]. 2.5 displays how the data concentrator servers[2] connects the meters with the head-end system. Data collectors acts as an interface between the AMI network and customer systems and appliances within the customer facilities.

2.2.3 Head-end System (HES)

The AMI head-end system (HES) are servers, part of a control system with a meter data management system (MDMS), usually located within the utilities' (DSO) network. Through the communication nodes, the head-end servers are able to communicate directly with the meters and vice versa. The relevant consumer data is collected and managed within the meter database system.

[2]Industrial IoT router with various OS, such as Linux or other

In most Smart Metering architectures, the head-end system or systems (HES) serves a dual purpose. The basic goal of HES is to automatically capture meter data while avoiding any human interaction, as well as to monitor parameters obtained from meters. HES is in charge of handling connectivity and data collecting from the metering infrastructure, which includes both meter devices and communication. HES allows for secure access to meters for purposes like as configuration, software upgrades and updates .

2.2.4 Communication networks

The AMI design requires separate communication networks for different purposes to achieve the two way of communication. Each with its own set of criteria and limitations, which were covered in 2.1.3: Home Area Network (HAN) for energy management at the consumer level, Neighborhood Area Network (NAN) collecting meter data from all meters in the "neighborhood", and Wide Area Network (WAN) for communication between all components of the Smart Grid. The NAN connects the HAN to the WAN. The NAN is comprised of smart meters, and the information gathered sends to the data concentrator which sends it further to the HES through WAN. Given the massive volume of data collected by data collectors across numerous WANs, a high transmission data rate is required at the WAN level.

2.2.4.1 Communication Technologies

As previously mentioned, the Smart Grid comprises a range of communication technologies to support the network architecture for electric power transmission and distribution, as well as consumer domains. This section gives a brief description of some of the communication technologies used within the Smart Grid network architecture, on the service providers' side, and in homes [22]. Here, we look at the entire Grid, but with a focus on AMI.

The communication technologies are categorized based on what medium they utilize to establish the connection. In Smart Grid communication systems, there are both wireless and wired communication technologies. Different communication technologies are suitable for different purposes in the system applications regarding requirements and properties. In some instances, wireless communication has advantages over wired technologies, such as low-cost infrastructure and ease of connection to difficult, unreachable areas and environment-threatening conditions. In other cases, the application of wired technologies is more appropriate.

The first flow is from the sensor and electrical appliances to smart meters in the two-way communication flow. The second connection is between smart meters and utility data centers. HAN to NAN, and NAN to WAN. The first data flow (within HAN) can be accomplished through powerline or wireless communications, such as ZigBee, 6LowPAN, Zwave. For the other information flow, cellular technologies or other wireless technologies are used. The technology choice that fits one environment may not be suitable for the other. In the following, some Smart Grid/AMI communications technologies, along with their advantages and disadvantages, are briefly explained [22] [62].

Power Line communication(PLC)

communication technology used for the transmission and distribution of data over power cables. They are mostly used for indoor environment [4] [60][62].

Wireline Network(Wired Communication)

transmission of data over physical filament - wires or cables constructs wired networks. Wired networks require extra investment in cable deployment. The advantages of wireless communication are that wired networks are more reliable in terms of security, higher communication capacity, shorter communication delay because there is no collision between packets. Wired networks are often the "backbone" of wireless networks [62].

- **Fiber Optic Networks** is an essential part of communication technologies in Smart Grid applications and can be applied both wired and in a wireless manner [20]. Fiber optic cables are data pipes that transmit pulses of light-down fibers thinner than a strand of human hair. Fiber optic is commonly known for enabling high-speed Internet, cable TV, and telephone service. The cables can link up smart meters and home gadgets that are designed to communicate with energy providers. Optical fiber has high speed and is considered one the best transmission medium for applications in Smart Grid, as it is suited for a long-distance network with a limited number of access points. High installation and monitoring costs are its major drawback. The downside of fiber optic is the costs associated with installation and monitoring. [7].

Wireless Network

In many cases, wireless networking technology has replaced the installation of wired networking. Advancement in wireless networking technology has enabled us to connect devices wirelessly, eliminating the installation of wirelines. In general, wireless signals are significantly subject to transmission attenuation and environmental interferences. As a result, wireless networks usually provide a short-distance connection with comparatively low data rates. Various protocols for wireless technologies in Smart Grid are mentioned in the sections below

- **ZigBee** is based on the standard IEEE 802.15.4, which defines the operation of low-rate wireless personal area networks designed for use in smart-home area application control systems. It measures energy consumption and enables both customers and utilities to monitor and manage customers' energy use. Smart meters have ZigBee chipsets to communicate with smart devices in the home. As sensors and controls do not necessarily need high bandwidth but rely on low latency, low energy for a long time, and long battery lives, ZigBee is suitable for this application. Short-range means 10 to 40 m, but mesh topology design lets the network cover larger areas [29][63]. The downside with Zigbee is the small memory size, and its interference with appliances that share the transmission medium can result in communication channel corruption.[35] Security is applied by default at the network layer, but higher-level security is optional and not required. Low cost, low power usage, mesh networking, and strong vendor support, ZigBee has many attractive characteristics for a smart home network that can easily attach to a smart meter for total integration. However, its security issues may be a cause of concern. As its importance and use increases, more and more threat actors are attracted to attacking it, exposing even more problems. In order to use ZigBee for complete power control from the utility, the smart meter will need to share keys with the homeowner's various appliances. However, due to security concerns, it remains to be seen if the utility would be willing to share these keys, possibly making system integration difficult [62].
- **Wireless Area network, WLAN*(IEEE 802.11)*** is known as Wi-Fi, is based on 802.11 IEEE series standard. WLANs are designed to provide a wireless access network with a radius between 150 - 250 meters [4]. These networks are mostly used in homes, offices, campus environments, and public areas like restaurants, shopping malls, and cafes.

WLAN uses IP protocol to communicate over the network with other appliances in the HAN[4][31][35][62].

- **WiMAX*(IEEE-802.16)*** is a standard for wireless technology that provides high-speed coverage up to 50 km and can be used by various applications. WiMAX support two-way real-time communication flow between nodes, which is why it is appropriate for applications used in Smart Grid: smart metering, distribution, and monitoring of transmission. Using bi-directional WiMAX links, outages are quickly detected, and power restored, resulting in increased reliability of the power supply. Finally, sensor data can be transmitted over WiMAX links for monitoring purposes [4] [35].

- **Cellular network** 2G, 3G, and Long Term Evolution (LTE) are potential cellular communications technologies used for Smart Grid communications. LTE has two key applications in Smart Grids, which are related to controlling and automation of distribution system and smart meters[4][35]. Cellular networks can be used for Smart Grid application purposes because they can save additional time and building costs for designing a dedicated infrastructure. Cellular networks are divided into different generations, such as 2G, 3G, 4G(LTE), and the upcoming 5G. Some of the features of current cellular networks are robust security, widespread coverage, low maintenance cost, and higher data rates [35]. Two cellular network technologies widely used for AMI purposes are LTE-M and NB-IoT - these are developed to fit IoT applications: NB-IoT is best for low-bandwidth, infrequent communication from a relatively fixed device, while LTE-M is a better fit for higher-bandwidth, mobile, or roaming applications.

- **Satellite** is a communication technology that transfers signals between two nodes. The signal is sent to the satellite, and the received signal is amplified and sent back to earth. The technology is used for radio and television broadcasting, communication to planes, ships, vehicles, and handheld devices. It is possible to provide coverage to every part of the earth that is not viable for other technologies with satellite communication. For Smart Grid applications, this technology can be used for remote monitoring of distribution and generation units. This is the only viable method to use where wired and other wireless communication technologies are available. Satellite communication has disadvantages for very high operation costs, and buying or renting a satellite on

space is not viable. Signals will take a long time to complete a round trip from the earth to space and back to earth. Weather conditions also affect the signal quality in satellite communication [4]. Satellite systems provide the widest coverage for WWAN environments. Broadband WWAN access technologies mainly consist of satellite networks that cover the world completely or partially. While they can be used as separate data networks, they can also be a backbone network for multiple WMANs in physically distant areas and less populated places not covered by WMANs. Different WMANs can communicate with each other via these backbone WWANs [31].

- **Bluetooth***IEEE 802.15.1* is a common wireless communication technology system where data is exchanged over a radius of fewer than 10 meters. Bluetooth supports a limited number of nodes that can be a serious constraint when having multiple devices in a HAN. Like many other technologies, Bluetooth is operated at low power, which means the strong noise can cause signal loss or damage. Moreover, it works on 2.4GHz and has interference issues with other wireless technologies such as Wi-Fi and ZigBee, placed with the same system frequency. Bluetooth has some inherent security issues and offers weak security compare to other standards [45][62].

Chapter 3

Theory

This chapter presents the threat landscape and security challenges in the AMI components we introduced in the previous chapter: *smart meters, data collectors head-end systems, and the communication network*.

Both cellular networks and human behavior are two factors that significantly affect the security of a system. Further in this chapter, we explain different methods to exploit cellular communication and human nature and the consequences of such attacks.

3.1 Security challenges AMI

Advanced metering infrastructure consists of unique properties. The two-way communication between AMI components incorporates the real-time exchange of private and sensitive data, vital control and safety commands, and utility providers' private information makes it a critical point in the power delivery system of valuable data [2]. Hence, utilities need a secure and flexible two-way communication infrastructure to connect and communicate with both the customer and enterprises [46]. Methods of breach of defense and exploitation of weaknesses in computer systems or networks challenge the security aspects of AMI. AMI has several points that are prone to attacks: hardware (smart meter, data concentrator), communication networks (HAN, NAN, WAN), data (database storage, data in transmission to utilities). These components pose different vulnerabilities.

Attacks on AMI could lead to power outages, e.g., by cutting off household electricity and over-loading the Smart Grid. In addition, if security breaches were to occur or vulnerabilities in threat actors exploit the systems, disruptions could be caused and create an imbalance in the processes. The worst-case scenario could be that the whole Grid is brutally affected, damaging

equipment, causing physical harm to individuals utilizing the Smart Grid. The consequences of such failure could lead to blackouts for cities or nations, and human life is endangered.

As a result, AMI are vulnerable to many cyber attacks from different threat actors with malicious intent, including illegal and unauthorized customers, insider attacks, organized criminal and terrorist groups, business competitors, and even nation-states actors (APTs).

The smart meter is, as mentioned in 2.2, an essential component of the Smart Grid. However, AMIs are usually composed of many smart meters installed in physically insecure locations and use insecure wireless communication easily corrupted.

Smart meters are being deployed globally, and statistics show that as of the end of 2019, the average global penetration of smart meters was 14% 3.1. Figure 3.1 show that Europe and the North-American continent are leading when it comes to the deployment of Smart Meters. With the global rollout of the 5G-network, the number of deployed smart meters will increase significantly, side by side, like other IoT devices

As the number of smart meters increases exponentially, security issues associated with Smart Grid and AMI grow substantially from within the system and outside.

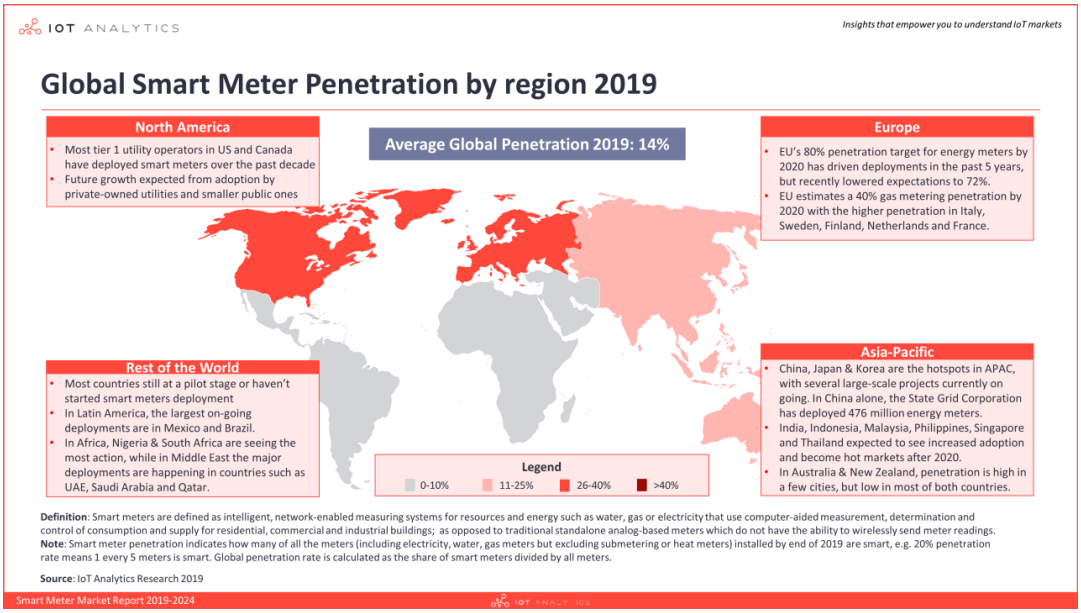

FIGURE 3.1: Smart Meter Market November 2019

Consumption data is critical and can expose the customers' daily patterns. Data transmitted over long distances and stored in various locations in the infrastructure creates vulnerabilities related to data theft or manipulation. The price signal and commands received at the consumer end are also potential areas for a cyber and physical attack to espionage, damage infrastructure, or power theft. [41] discusses topics related to AMI and consumers' perspectives. The following is stated *Consumers' peace of mind is critical in the success of smart meters and the expansion of AMI. If consumers believe that their data is used against their will or experience poor service or power quality due to external manipulation of the system by unauthorized parties or hackers, they most likely resist the implementation of AMI. Potential health hazards and higher bills after installing such intelligent meters will also affect the consumers' decisions. The go decision is taking these issues seriously and is working on procedures to guarantee customers' privacy of information. The government is also launching campaigns to increase the public's knowledge of smart meters and address their legitimate issues regarding health and cost. Utility companies, as well as installation technicians, are also playing an essential role in this regard*

3.1.1 Basic principles

Data security, information security, or IT security are all categories within a subject area linked to the fundamental concepts of cybersecurity: confidentiality, integrity, and availability *(CIA objectives)*. In most fields of cybersecurity, the CIA objects are used as a starting point for setting requirements. The same principles are applied in the case of Smart Grid and its components. [2] has mentioned some of the requirements that need to be explored, especially considering Smart Grid and AMI. *"Security-sensitive topics are typically discussed in the context of the so-called CIA triangle: confidentiality, integrity, and availability. Metering services are essential to ensure reliable energy provisioning, and meter readings are sensitive data whose protection is a major objective in future infrastructures"* [54]. Figure 3.2 shows the difference between how the principles are applied and also displays essential assets of Smart Grid.

The main goal of the attacks is to get unauthorized access to the devices and networks to challenge the main security goals of confidentiality, integrity, and availability. Access to the internal devices (e.g., smart meters, data collectors) or a compromised supply chain can be granted through physical or cyber domains.

For most systems, the importance of the three principles is in the following priority order: confidentiality (1), integrity (2), availability (3). For systems that are categorized as ICS, availability and integrity are the most important.

Confidentiality: is about preserving information from access and disclosure to unauthorized entities, processes, or individuals. In terms of AMI, confidential information could be metering information such as usage and billing details between consumers and entities. If such information is not protected, disclosure could lead to manipulation, modification, or be used for other malicious purposes [15].

Confidentiality in AMI is related to the privacy of consumption and other customer details. As for many other systems, data confidentiality in AMI can be ensured by using proper data encryption techniques such as symmetric or asymmetric encryption.

Integrity: is about protecting information from unauthorized alteration and ensuring that data is always reliable and correct. The need to safeguard information includes data stored on systems and data in transmission between nodes. In AMI, the flow of information that transports energy consumption data is used for accounting and billing must not have tampered with. Proper protection mechanisms must be in place to prevent the manipulation of the smart meter device. The injection of tampered wrong status messages in the communication network might cause problems in network management and affect the data and commands send back and forth from the meter. Attacks that compromise AMI's integrity might result in loss of control of the Smart grid by utilities. Non-repudiation and authenticity of information are required to maintain integrity in the information flow [15][26].

Availability: the information must be available to authorized entities upon demand. Because the loss of availability means disruption of access to systems and services, in the ICS, availability is considered the most important principle. Therefore, the focus is less on the information and more on the industrial processes that information technology controls, ensuring systems stay up and running and avoid interruptions or unexpected downtime. Power is an essential part of modern life and important to economy.

In AMI, availability concerns are twofold [54]:

1. From the consumer's point of view, power availability is most important: no one should accidentally turn off electricity or maliciously.

2. From the utility perspective, remote meter accurate readings on time are essential to prevent energy theft and keep the business running. In addition to recording and sending meter usage, smart meters send status messages (e.g., load calculations, blackouts) to the utility and monitor the Smart Grid situation. If any nodes fall outside the network, smart meters will notify utilities and reconnect with other nodes. Hence the availability of smart meter communication must be running.

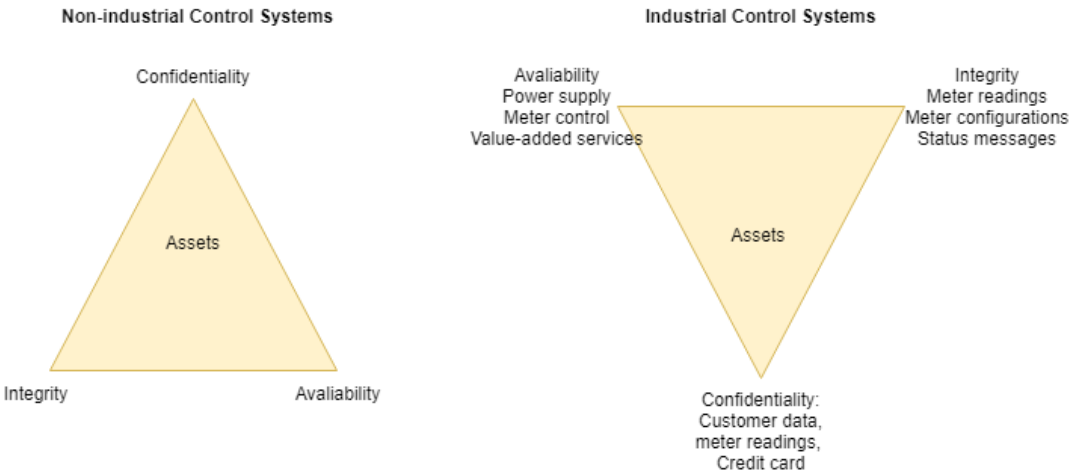

FIGURE 3.2: CIA and AIC

3.1.2 AMI Attack Surface

To assess the various vulnerabilities inside the AMI, we used many research articles. We've used the following: [11], [37].

3.1.2.1 Smart Meter

Although smart meters help improve the entire grid process, the meters and their network introduce new security issues expanding the threat landscape. Studies we have used as references in this thesis, such as [11], [37], and [38], are a few of many that throw light at the fact that deployment of smart meters raises significant security concerns. The concerns are related to consumers' privacy, data integrity, authentication, access control, and system availability.

The authors of [53] consider smart meter as the weakest link in the Smart Grid in terms of possible security breaches due to many cooperating technologies, communication over different channels and networks, and lack of proper security measurements. The smart meter can be exploited through both the physical and digital space. The consequences of an attack on a

smart meter can destroy both hardware and software. [53] explains that smart meters are easier to attack through the wireless networks HAN, NAN, and WAN, which we will look at in 3.1.2.4. Installed at consumers' sites the smart meter is easily accessible - in homes or, e.g., common areas of apartment complexes, such as in a room downstairs in basements accessible by the residents and other parties [1]

A summary of some of the vulnerabilities that the smart meter poses:

- Physically accessible to the public
- Poor communication protocols and channels

3.1.2.2 Data Collectors

Connecting multiple smart meters together, a security breach would impact a large amount of consumers. Both physical and cyber attacks can compromise the data concentrators. The physical attacks occur due to the data concentrators' availability to more people than those who are actually supposed to have anything to do with it. The alteration to its hardware would allow malicious software to be installed on the could infect any smart meters linked to it.

The GPS receiver[2] synchronizes all of the AMI components' data as well as time and date. Manipulating the HW would have an impact on the precise timing of infrastructure configuration, message transmission, and billing for consumers. USB port allows the attacker to simply install malware using the USB flash drive. Interrupting the data collector would impact the connected smart meters as well, and have further impact on the meter data management system. Attacks on the concentrator could result in data theft, power theft, denial of power, and interrupting the grid.

A summary of some of the vulnerabilities that the concentrater poses:

- Physically accessible to the public, and poor security mechanisms
- OS is often well-known by hackers. Linux based etc.

[1] At many given addresses in Oslo, it is very easy to reach the smart meters. In several places, especially at apartment complexes, the meters are installed in bundles basements that many people has a key to

[2] A GPS Receiver is a L-band radio processor capable of solving the navigation equations in order to determine the user position, velocity and precise time (PVT), by processing the signal broadcasted by GPS satellites [19]

3.1.2.3 Head.end System

HES is usually located at DSO, and is therefore exposed to the inside threat from people working at the utility, and other cyberthreats that a company experiences (i.e. spear-phishing, supply-chain attacks, ransomware). Security holes in the WAN can also threaten the systems. As MDMS contains private data and must be secured.

3.1.2.4 Communication networks

With AMI's significant usage of wireless protocols, cyberattacks become more likely, and the system becomes more vulnerable. Despite the fact that these protocols have been in use for a long time and are extensively used, they remain the primary target for cyberattacks against Smart Grid infrastructure. Some of these protocols include insecure encryption and key exchange methods, putting data integrity and the system at risk. [3] proposes the vulnerability surface of the Smart Grid, that are also relevant for AMI. We look at these vulnerabilities from an AMI perspective:

1. Wireless networks are available everywhere from anywhere
2. AMI is comprised of a variety of network technologies that operate on various channels, protocols, and subcategories of communication technologies that are tailored to certain applications. This implies that, in addition to the vulnerabilities inherited, there is much to maintain and keep in track of.
3. Using Internet Protocol (IP) and commercial off-the- helf hardware and software: Using IP standards in smart grids offer a big advantage as it provides compatibility between the various components. However, devices using IP are inherently vulnerable to many IP-based network attacks such as IP spoofing, Tear Drop, Denial of Service, and others [3].
4. Implicit trust between traditional power devices: Device-to-device communication in control systems is vulnerable to data spoofing where the state of one device affects the actions of another. For instance, a device sending a false state makes other devices behave in an unwanted way (i.e Meter to Meter communication, meter to head-end) [3].
5. Greater number of intelligent devices: A smart grid has several intelligent devices that are involved in managing both the electricity supply

and network demand. These intelligent devices may act as attack entry points into the network. Moreover, the massiveness of the smart grid network (100 to 1000 times larger than the Internet) makes network monitoring and management extremely difficult [3].

AMI's communication network is very vulnerable to both traditional network attacks, but also new attacks that are introduced parallel to the development of IoT.

3.2 Compromising cellular networks

The primary technology for connecting people with people, people with devices and devices with devices, are cellular communication. The infrastructure of cellular communication networks is massive and complex. The complexity of billion nodes connected to a system presents a challenge when providing security in every possible communication path. The section below will look at the application purposes of cellular communication, more precisely, the application in the Internet of Things domain. Our main goal is to examine present vulnerabilities in mobile communication and attack techniques that could exploit these vulnerabilities. Chapter 4 will look more closely at attacks that compromise AMI with cellular communication as an attack vector, and address these in depth.

3.2.1 Cellular communication: an overview

Cellular communication, also referred to as *mobile communication* [39], are wireless communication networks applied for data transmission purposes. Cellular communication has become increasingly important due to the growth in the number of gadgets and devices that depend on Internet connection, irrespective of the object's location. According to many researches, there is yet no standard single solution that is ideal to fit all the different type of IoT applications. As a result, the mobile industry is standardising several cellular communication technologies, including Long Term Evolution for Machines (LTE-M) and Narrow Band IoT (NB-IoT) that we mentioned previously.

3.2.1.1 Applications of cellular communication

The interconnection of communication networks and the Internet significantly expand the availability of cellular communication to telecommunications subscribers. Cellular networks serve many indoor and outdoor devices and cover technologies across industries and businesses. These systems, which used to be confined to basic phone services, now enable data connections at the lower end of the broadband spectrum. As a result, devices connected to such networks may participate in a wide range of applications, from standard phone calls to streaming video.

The current mobile communication approaches focus on the Smart City concept and the growing Internet of things (IoT) trends. We have summarized

a few of the many applications of cellular communication in figure 3.3 and chosen to explain a few of them briefly. We can deduce from the figure 3.3 that many important services and tasks in society and critical infrastructure is dependent on mobile connections.

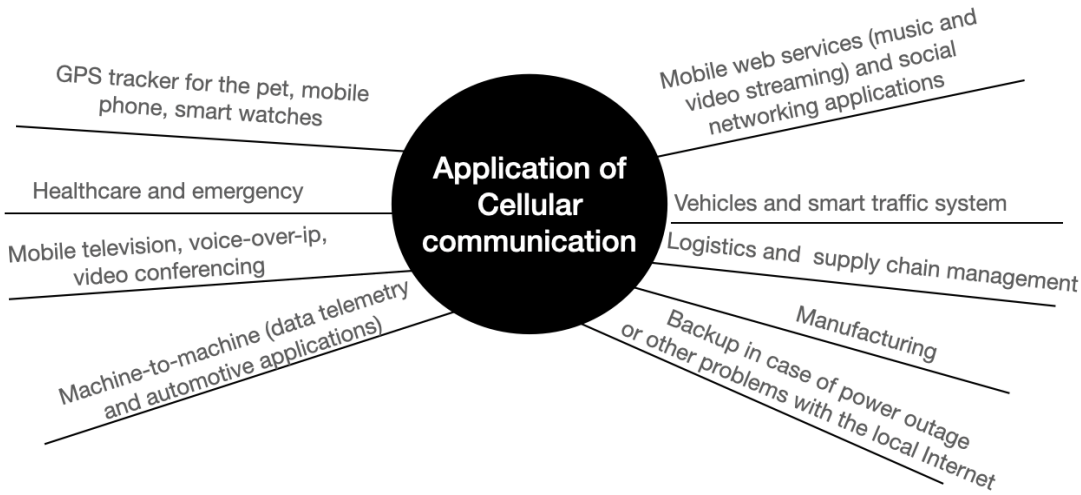

FIGURE 3.3: Applications of Cellular Communication

Modern vehicles and road traffic systems are heavily dependent on cellular communication. Intelligent vehicles use mobile connections for mapping, navigation, voice recognition, bug reporting, software updates, entertainment, and many other things. Cellular connection is necessary for the smartphone app to remotely unlock the car and sound the horn, charge, AC, and locate the car. A mobile connection network is also used to fast exchange information such as distance between two vehicles, traffic information, road conditions in emergencies, or help each other keep a safe distance.

Cellular communication is widely established in machine-to-machine (M2M) communication between two or more technical entities to achieve In addition to NB-IoT, LTE-M, or 4G/5G technologies, the Smart Grid is one of the many application sectors of M2M communication. Cellular IoT connections are primarily divided into two types: LTE-M and NB-IoT, which are recent IoT-specific features customized to the demands of IoT devices and applications. IoT components may be connected using 2G, 3G, 4G, and 5G networks. 2G and 3G however, are not deployed for mobile communication. Other countries, on the other hand, continue to use these connections for smart devices like parking meters.

3.2.2 Security challenges

Communication security involves safeguarding the communication process and data flows. The massive and complex infrastructure of communication networks with innumerable entities coordinating, communicating, and transferring massive data presents a challenge for the network to provide security at every possible communication path. With cellular communication serving many important aspects of the digital domain, proper security countermeasures are essential to protect the major data traffic flows. It is the practice of limiting access entries to telecommunications by unauthorized interceptors while still providing material to the intended receivers and decreasing the risk of unauthorized disclosure to the outside world.

Several factors may influence security and increase the chances of a communication network attack. In a mobile network, the growing number of subscriber, such as computers, processes, and people raises vulnerabilities and broadens the threat surface. Every wireless network is inherently susceptible since the connection is broadcast over the waves and may be accessed by anybody within the range and with the right toolbox. To guarantee that the proper individuals are using the network, the system must authenticate each subscription. The issue of cross-region and cross-provider authentication becomes a concern since the goal of mobile is to enable people and machines to interact from anywhere in the globe. Many components provide functionality accessible through a web service. Web services, web interfaces and standard open web protocols, such as HTTP, lower the entry barrier for the operators and the hackers. Due to standard channels and common communication technologies, a zero-day found in one channel could be used to attack the same devices or other entities using the same protocols or channels. The actual location of a cellular device needs to be kept hidden for the user's privacy and for the hardware to be unavailable to the public. With IP networks and location tracers, issues related to location being disclosed arises. The users' association to an access point might disclose information about their location. In the case of a device being lost or stolen, potentially sensitive information can fall into the hands of unauthorized parties. More comprehensive functionality specs in cellular communication systems mean the broader landscape of malware and viruses injected in the communication. An infected device can also be used to attack the network infrastructure from the inside. With wireless networks generally, the threat landscape is

much broader compared to wired networks, as the network practically is accessible to anyone, anywhere. The vulnerabilities mentioned in this section and the attacks presented in the following sections are not limited or unique for cellular communication but many other wireless networks.

3.2.3 Cellular communication: An attack vector

Due to the massive architecture of cellular networks, there are a variety of attacks that can compromise the communication infrastructure. We have chosen to look at a few of the most popular attacks and how they are used to compromise cellular networks (and wireless networks in general). The bullet summarizes entry points in a cellular network, figure 3.4 illustrates the points visually.

- Compromise to the IoT device and system supply chain
- Weak device authentication by the network and user authentication by the device
- Misconfiguration on the device or in the network
- Theft or modification of data-in-transit or data-at-rest
- Distributed Denial of Service (DDoS) attacks against the network or cloud applications
- Malware infection of devices, including viruses, bricking, bots, and ransomware
- Command and Control (C&C) botnets in which devices target cloud applications and external networks
- Unauthorized access to a cloud application leading to data breach
- Unsolicited traffic from the internet destined to the device

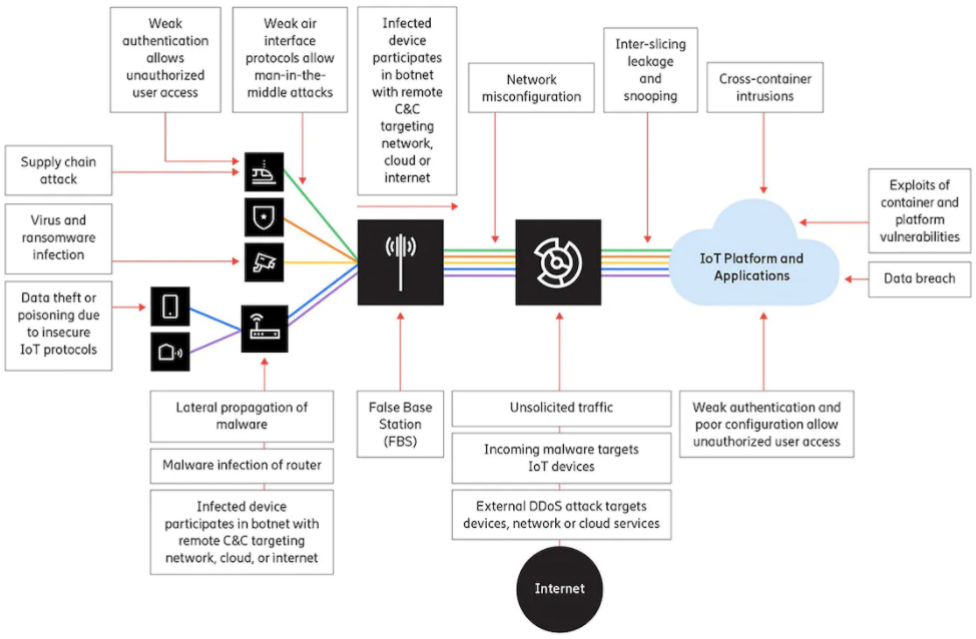

FIGURE 3.4: Cellular communication network [47]

3.2.4 Cellular communication: An attack vector

Due to the massive architecture of cellular networks, there are a variety of attacks that can compromise the communication infrastructure. We have chosen to look at a few of the most popular attacks and how they are used to compromise cellular networks (and wireless networks in general). In the following sections, we present possible entry points in the network exploiting different vulnerabilities. Due to many weaknesses in the network, as the figure above shows, there are many different entry points in the network. Different attacks uses different entry points in order to exploit the vulnerabilties.

3.2.4.1 A definition: passive and active approach

Technical cyberattacks can be categorized into active and passive attacks, depending on how they are carried out. Because we use the terms active and passive regarding the attacks outlined below, we have decided to go through the definition of passive and active briefly.

Passive attack is a network attack where the data flow of a system is analyzed, and the system is checked for open ports and vulnerabilities. The goal is to gather knowledge about the target system without taking any active

steps against it without affecting or changing the system resources. These kinds of attacks are typically applied before a more active attack.

Active attack is a network exploit where an attacker actively engages in changing, modifying, and compromising system resources. In other words, an active attack refers to "hacking" activities.

3.2.4.2 Denial-of-service (DoS) and distributed denial-of-service (DDoS)

DoS and DDoS compromise the availability of system resources that must be accessible and available to an authorized entity (process, system, person) on demand. DoS-attack involves a system attacking another system, while the DDoS, on the other hand, involves several systems attacking a single system.

There are several forms of denial of service attacks and many techniques that affect the availability of a system. We will look at some of these techniques that are applicable to wireless cellular communication networks:

Rouge device is a malicious device. A common denominator for all rouge devices (be it a mobile phone, access point, smart meter) is that they exist for the sole purpose of stealing information, disrupting network operations, or causing harm to the network and systems. The device can become rouge due to several reasons. Misconfiguration, incorrect, or lack of patching could lead to vulnerabilities being exploited. A threat actor could infect the entity with malware. Rogue wireless nodes is one of the common security threats in wireless networking.

A rogue device facilitates these devices to carry out MITM attacks by spoofing the data packets transmitted across the network. They may also be used to carry out DDoS to overload the network attacks by establishing a botnet that sends massive amounts of data and numerous data packets to the network.

Flooding attacks are categorized as DDoS. The concept is to send a massive amount of traffic (flood) to a particular server or a service, aiming to exhaust all the resources trying to respond to bogus traffic so that it cannot process legitimate requests for service or send a massive amount of traffic onto a specific network segment with the goal of creating so much network congestion that legitimate traffic cannot reach the target server or service. There are different types of flooding attack. [5] describes SYN flooding attack and ICMP flooding in the following way:

- *"SYN flooding is one of the most popular flooding attack. SYN flooding exploits the weaknesses in the Transmission Control Protocol (TCP). SYN packet in TCP is required to establish a connection between any two hosts. It is a request sent by the host to make a connection. Attackers send SYN packets to the ports that are in the 'Listening' state in the target host, these packets have a source address that does not represent the actual host. The target responds with a SYN or ACK packet addressed to the source address in the SYN packet that was received. As the system does not exist and the source address was invalid, the target keeps waiting for a packet acknowledgment to complete the connection process. The allocation of resources by the target in response to these malicious packets leads to a DDoS attack."*
- *"ICMP flooding attack exploits configuration errors on the involved network devices involved. It lets packets to be sent to a network via broadcast address, which were to be sent to a specific host. The attacker sends a large number of IP packets with an invalid source address. This leads to network bandwidth drainage, causing legitimate packets to be blocked. There is also UDP (User Datagram Protocol) flood attack which exploits the connectionless TCP/IP stack protocol to generate a DDoS attack. Using UDP for DoS attacks is not as straightforward as with TCP. A UDP flood attack can be initiated by sending a large number of UDP packets to random ports on a destination host and forcing the destination host to send a large number of ICMP packets."*

3.2.4.3 Man in The middle (MitM) attacks

Briefly explained, man-in-the-middle is a type of attack where communication between two entities is intercepted *(breaking confidentiality)* and potentially changed *(breaking integrity)* by a third-party, also known as the man-in-the-middle. We will have a look at some type of MitM-attacks in the paragraphs below that appear quite frequently in wireless technologies. MitM-attacks are commonly used to overcome security systems in order to spread malware such as viruses, bots, keyloggers, ransomware, and other malicious software.

NAN-sniffing aims to break network encryption, disclose the communication protocol, and learn about data formats and message types transmitted over the network. This is a type of eavesdropping, and the attack's success depends on the topology and technology of the infrastructure (e.g., dedicated channel or shared IP channel). NAN sniffing would be the first step in a multi-staged attack and, thus, the basis for active manipulation of own or

foreign devices [55]. The authors of [55] explain NAN-sniffing on AMI which we will look into later in the thesis.

Relay attack is a very *IoT-specific* attack, that "involves placing an illegal device between the reader and the tag in such a way as to intercept the information between the two nodes and then modify or transmit them directly to the system. The information transmitted by illegal devices will encounter a certain delay, and therefore these attacks are called relay attacks" [1].

3.2.4.4 Routing attacks

By forging or retransmitting routing information, an attacker may create routing loops to resist data transmission, increase or decrease the path length, generate error messages, increase network latency, or capture or repel network traffic. Other routing attacks are included in the following. There are different type of routing attacks [50]:

A wormhole attack: This is a form of network layer attack in which more than one rogue node is used. The nodes used in this attack are more advanced than typical nodes, and they can create better communication channels over longer distances. The aim of this attack is to send data through a tunnel from one compromised node to another compromised node on the other end of the network. As a result, other nodes in the network may be led to believe that they are closer to other nodes than they actually are, causing routing algorithm difficulties. The data packets may also be tampered with by the infected nodes.

Sinkhole attack are carried out by either compromising a network node or establishing a rouge network node. The malicious node presents itself as the quickest link to the base station and attempts to direct traffic away from other nodes. This draws all nodes around the sinkhole. The data can thus be readily altered by the attacker node or the sinkhole.

Botnet attack Botnets are created by infecting connected devices with malware and then controlling them through a command and control server. Once a device on a network has been hacked, other devices on that network are at risk of being infected.

A botnet is a collection of computers (connected to the Internet), i.e routers, that have been infected with malware, and are now under the control of hackers. These machines can attack in different ways, they could initiate DDoS against targeted companies in order to disrupt their operations and services.

A botnet can also be used to conduct cyber espionage to steal sensitive information. The amount of devices that make up a botnet determines how powerful it is. The botnet malware families that infect devices demonstrate the threat's nature: They're made to collect as many devices as possible while avoiding other botnet viruses.

3.3 Compromising human behaviour

Even when security measures are implemented correctly to prevent machine-based attack methods, humans can give threat actors everything required to exploit a system. Social engineering is the art of exploiting human behaviour, Social engineering is human hacking. The *hacking* techniques are based on bypassing the security measurements and compromising the security principles (e.g., confidentiality, integrity, availability) by establishing a relationship with the user and getting users themselves to divulge information that can harm systems. This technique is often a highly targeted approach and targets humans with access to specific data and information, which is of interest to a threat actor *(here: social engineer)*. The social engineer (SE) would manipulate humans in different ways into disclosing confidential information or even into carrying out their malicious attacks through influence and persuasion without victim(s) knowing that they are leaking information or causing harm to the systems. The information may be used to gain initial access to systems or as a part of other hacking events. A social engineer is not necessarily a hacker but a hacker enabler by definition.

In terms of information systems, the ultimate goal of the SE is to gain access (either physical or digital) to information or information systems. The process is roughly the equivalent of trespassing and, perhaps, even breaking depending on the methods used. [59] describes a social engineering scenario as following:

> *Someone calls claiming to be from computer support and says, "Hey, this Chuck from support, and we need to check the network's connectivity. What's your login and password?"*

While this may be an exaggeration, the basic framework is set:

> *"Hi, I'm someone you should trust, and I sound like I know what I'm talking about, and I'm working on something you probably do not understand. For those reasons, I need you to give me a piece of information that you normally wouldn't give to a stranger, but hey, I'm legit."*

With the information collected, the SE can enable a hacker to penetrate the system to extract, modify, or destroy the information and cause disruption in services. Technical protection measures can protect the system to some extent but have in many cases proven to be ineffective against this kind of attack as shown in 3.3.3.

Social engineering is superior to most other cyberattacks because it can breach even the most secure systems. The users think they are the hardenest security layer, but many studies state that human is the weakest link [56][34]. In many cyberattacks compromising humans have been the input factor. Lee Ferran stated that *"No matter how sophisticated the attack or how capable the defenses, the weakest link in cybersecurity is often the human at the keyboard"*. Research and many real-life examples have shown that social engineering is easy to automate in many cases and can be performed to a large extent. Social engineering has become an emerging threat in virtual communities [30]. It has high proven to have high damage potential in the digital domain, including critical infrastructure and attacks on the Smart Grid architecture.

3.3.1 The Human Factor

Social Engineering, in the context of Information Security, is a threat to Privacy, as it is the psychological manipulation of people into performing actions or divulging confidential information. Social Engineering is a type of confidence trick for the purpose of information gathering. An essential part of successful social engineering attacks is social approaches. Accordingly, attackers depend on socio-psychological strategies such as Cialdini's principles of persuasion to manipulate and control their victims. Cialdini's Six Principles of Persuasion are termed: Reciprocity, Scarcity, Authority, Consistency, Liking, and Consensus. Cialdini's writing was aimed at salespeople, recruiters, advertisers, and marketers, or summarized as professional players in the field of communication [10]. The principles are also applicable to cybersecurity, as they play a crucial role in social engineering [30].

- Reciprocity – the act of exchanging goods and services with others for mutual advantage People often believe that if someone does something nice for them, they owe something to them to repay the favor.
- Commitment and Consistency – When people verbally or in writing commit to an idea or goal, they are more likely to follow with it because they have acknowledged that the idea or goal corresponds to their self-image. Even if the original motivation or purpose is removed after they have already agreed, they will continue to fulfill the deal.
- Social Proof – People tend to do things that they see other people are doing.

- Authority – People are more likely to obey those in positions of authority.
- Liking – People are easily persuaded by other people whom they like.
- Scarcity – Perceived scarcity will generate demand.

In the example above one can see at work both the Authority principle, as the one calling pretends to be an authority in the technical aspects that the user does not know about, as well as the Reciprocity principle, as the one calling offers something to the user, i.e., help with the technology, for which he asks something seemingly "little" in return, i.e., the login credentials. If the SE approaches the victim also at a special moment, such as when the user experiences real problems with the technology, then this becomes an application also of the Scarcity principle, since the SE is seemingly providing something in high demand, i.e., technical help. Cialdini does not explicitly mention curiosity as one common social vector, but in social engineering this is much used in spear-phishing and baiting attacks. To increase the chances of a successful attack, the SE often tries to develop a relationship with their future victims, i.e., applying the Liking principle.

3.3.2 Cyber Kill Chain

To understand how social engineering takes part in a hacking sequence, we must look at some concepts related to the structure of a cyberattack. In many sophisticated attacks, an adversary performs several stages to conduct an attack. We will in this section look at stages in which social engineering is part of, specifically attacks that can be performed on AMI.

The figures 3.5 and 3.6 give a representation of the stages in an attack that can include steps of social engineering. For the Smart Grid, in general, and as shown in 3.5, there are, according to [15], four steps used by malicious hackers to attack and gain control over a system: reconnaissance, scanning, exploitation, and maintain access. The Cyber Kill Chain, by Lockheed Martin, models and analyzes actions of an attacker: *reconnaissance, weaponize, delivery, exploitation, installation, command, and control* and *act on objectives*. We have used Lockheed Martin's model in this thesis, as it is more comprehensive and detailed. In the first three steps of *reconnaissance, weaponizing, and delivery* social engineering is a heavy input vector. From *exploitation* and onwards, technical hacking techniques are used.

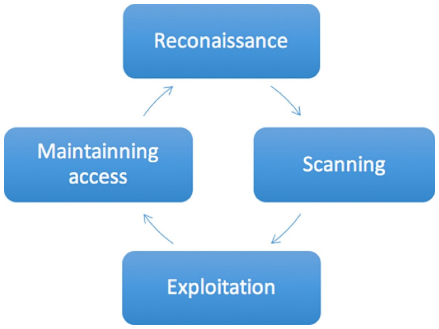

FIGURE 3.5: Smart grid Attacking cycle [15]

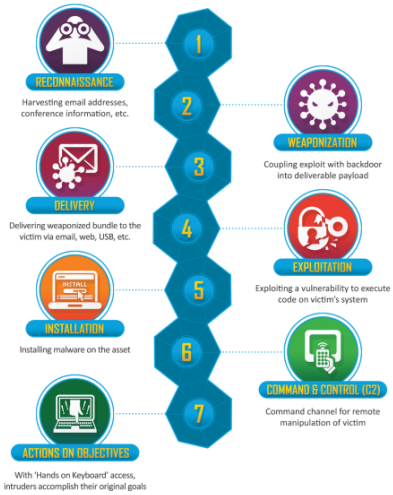

FIGURE 3.6: Cyber Kill Chain, by Lockheed Martin

Step 1: Reconnaissance

In this step, the attacker gathers and collects information about the target. The more time, work, and effort utilized during this phase, the more likely a hacker will succeed with the attack. Social Engineering is a common technique in this stage to acquire knowledge about the victim [15]. An attacker would use social approaches such as communication and persuasion to gain trust and get an overview of significant individuals and companies related to the system. A threat actor can apply different techniques to obtain the information needed to carry out an attack. Some steps a threat actor might perform:

- Scanning targets' social media platforms and profiles *(LinkedIn, Facebook, Twitter)*, search for related customers and other companies involved in the business, make fake calls or send fake e-mails to get more information. Phishing, impersonating, and dumpster diving are widely used during this phase.
- A more technical approach in this stage is to use system information to gain access to digital and electronic devices. System information can help bypass routers and firewalls, check for IP addresses, hosts, and domains, and learn which hardware and software are used. Google hacking and other commands are widely used and checking the information in directories and databases.

An example from [17]: *Let us assume you are conducting a penetration test on an organization. Early reconnaissance, you discover an e-mail address for one of the*

company's salespeople. You understand that salespeople are highly likely to return product inquiry e-mails. As a result, you sent an e-mail from an anonymous address feigning interest in a particular product. In reality, you did not care about the product. The real purpose of sending the e-mail is to get a reply from the salesperson so you can review the e-mail headers contained in the response. This process will allow you to gather additional information about the company's internal e-mail servers. Let us take our social engineering example one step further. Suppose our salesman's name is Ben Owned (we found this information during our reconnaissance of the company website and in the signature of his e-mail response). Let us assume that in this example, when you sent the employee the product inquiry e-mail, you received an automatic reply with the notification that Ben Owned was "currently out of the office travelling overseas" and "would be gone for two weeks with only limited e-mail access." A classic example of social engineering would be to impersonate Ben Owned and call the target company's tech support number asking for help resetting your password because you are overseas and cannot access your Webmail. If you are lucky, the tech support people will believe your story and reset the password. Assuming they use the same password, you now have access to Ben Owned's e-mail and other network resources like VPN for remote access, or FTP for uploading sales figures and customer orders.

Step 2: Weaponizing

In this phase, information acquired through reconnaissance is used to create cyber weapons to enter the network without interaction with the victim. Similar to the previous step, both social engineering and technical hacking techniques are applied in this phase. Social engineering-based techniques are used to create convincing and trustworthy spear-phishing e-mails and URLs. The e-mails might have the appearance to look like it is from a known a trusted party. The social engineer might attach an infected executable to the e-mail, or the e-mail might contain a malicious link. Sometimes as seen in 3.3.4.3, a trusted party's systems are compromised in order to get closer to the target, or perhaps the threat actor creates a self-replicating malware to be distributed via USB drive as mentioned in 3.3.4.1. Another social engineering technique used in this phase is watering hole attacks *(fake web page)*. Threat actors select the most appropriate legitimate sites to compromise. Instead of targeting random sites, the waterholes rely on trusted targets and relevant websites. The website might offer the victim a free download of a document or present something of interest to the victim. The purpose is to create a weapon that can capture personal credentials. The threat actor also

collects tools and programs that will be used when the network is accessible. Table 3.1 gives an overview of common and popular cyberweapons.

Cyberweapon	Description
Botnet	A network of computers forced to work together on the command of an unauthorized remote user. This network of robot computers is used to attack other systems
DoS	Distributed Denial of Service attacks is where a computer system or network is flooded with data traffic, so much that the system can't handle the volume of requests and the system or network shuts down
Malware	Malicious software is injected into a system or network to do things the owner would not want to be done, such as create backdoors. Examples include: Logic bombs, worms, viruses, packet sniffers, ransomware, spyware (eavesdropping on a network, keyloggers)

TABLE 3.1: Common Cyberweapons

Step 3: Delivery

The cyberweapons constructed in the previous phase are now launched, and the intrusion payload is through different methods transferred6596707 to the victim using social engineering and hacking techniques. The social engineering techniques, baiting, phishing, and water holes, are now launched. Phishing e-mails are sent, watering hole web pages are posted to the Internet, the attacker might even perform USB-baiting. The attacker waits for data to be fetched by the malware that the victim is tricked into downloading. In an adversary-controlled delivery that involves direct hacking into open ports, the goal is to install malware (a dropper) allowing attacker command execution or malware (a downloader) to download additional malware from the Internet, allowing attacker command execution[3]. It is important to note that although many technical mechanisms are used to stop an adversary-controlled delivery in this step, the human vector does play a critical role - a trained workforce significantly reduces this attack surface area.

Step 3: Exploitation

During this phase, the attacker exploits vulnerabilities in a system with cyberweapons. The malware collects the credentials such as usernames and

[3]Deloitte

passwords, and the hacker tries to log on to e-mail systems or bypasses VPN connections using these credentials. With the malware attachments sent through phishing, the attacker can remotely access infected computers, search through the network, analyze traffic flow, and further exploit the system. The ultimate goal is to establish a foothold inside the network and move laterally further. The attacker typically downloads additional tools on the victim's systems, attempts privilege escalation, and extracts password hashes to achieve the goals.

Step 4: Installation

In this phase, persistent backdoors are created, admin accounts are made, and mechanisms that offer security, such as firewall and IDPS (Intrusion Detection and Prevention Systems), are disabled. The goal is to move freely through the network and stay there as long as needed.

Step 5: Command and control

Now the threat actor has gained admin privileges. The tools and admin privileges allow the threat actor to access the network and control everything, whether impersonating or sending fake e-mails, further downloading of tools, or even interrupting services.

Step 6: Act on objectives

In this phase, the attacker is finally able to achieve the main goals. The goals vary by who the attacker is and what their intentions are. The attack's objectives could be disrupting services, stealing confidential product information, or destroying hardware/software. Considering Industrial Control Systems, hackers could gain access to the systems, shut down equipment, enter new setpoints, and disable alarms.

3.3.3 Social Engineering attacks

There is a wide range of social engineering attacks, completely technical, non-technical, and socio-technical. Below, we have chosen to briefly explain the attacks frequently used among hackers today and relevant for application on AMI. We elaborate these further in CH 4.

Social engineering attacks are multifaceted and include physical, social, and technical aspects that are used in different stages of the actual attack. This subsection aims to explain the different approaches attackers use. Table 3.2

shows the links between social engineering techniques, attack vectors, methods, and psychological factors, which help compromise a system successfully.

Technique	Attack vector	Approach	Psychology factor
Baiting	USB containing malware	Leaving an USB where target(s) will find it and use it	curiosity
Phishing	Email containing malicious links or attachments	Sending a legitimate-looking email to targets	scarcity, reciprocity
Water hole	Fake website	redirect victim to a fake website	authority, curiosity
Tailgating	Physical appearance	entry to a restricted area without proper authentication	politeness
Pretexting	Fake situation, persona	Impersonating, or creating a fake situation	authority, liking
Quid pro quo	phone, email	trade of service for information	politeness, authority

TABLE 3.2: Summary of Social Engineering Attacks

Figure 3.7 displays the different aspects of a social engineering attack and how everything is interconnected. The adversary is a social engineer attack could be an individual operating alone or a group of organized people performing this attack. The target could be a specific individual *(such as spear phishing)*, an organization, or a specific group of individuals *(such as phishing)*. The goal in this type of attack can vary, depending on the end goal. It could be everything from direct attacks financial gain, unauthorized access, service disruption, or collect data, harvest credentials or get initial access as the initial step in a sequence of steps containing different attack types. Social engineering attacks can be carried out in different ways. The most popular ones are phishing, pretexting, baiting, water holing, and Quid Pro Quo. One attack can contain many different attack techniques with direct communication between the social engineer and the target, or through indirect communication, using different mediums, all depending on the attack. One common thing for all social engineering attacks is that they are all carried out using psychological factors in order to hack the brain. The following paragraphs present attacks in social engineering.

3.3.3.1 Phishing

Phishing is the most common type of attack leveraging social engineering techniques. Emails, social media, instant messaging, fake websites are a few of many channels used to trick victims into providing sensitive information (credentials, passwords, usernames). Phishing attacks have been used in many sophisticated and advanced well-known cyberattacks and are often

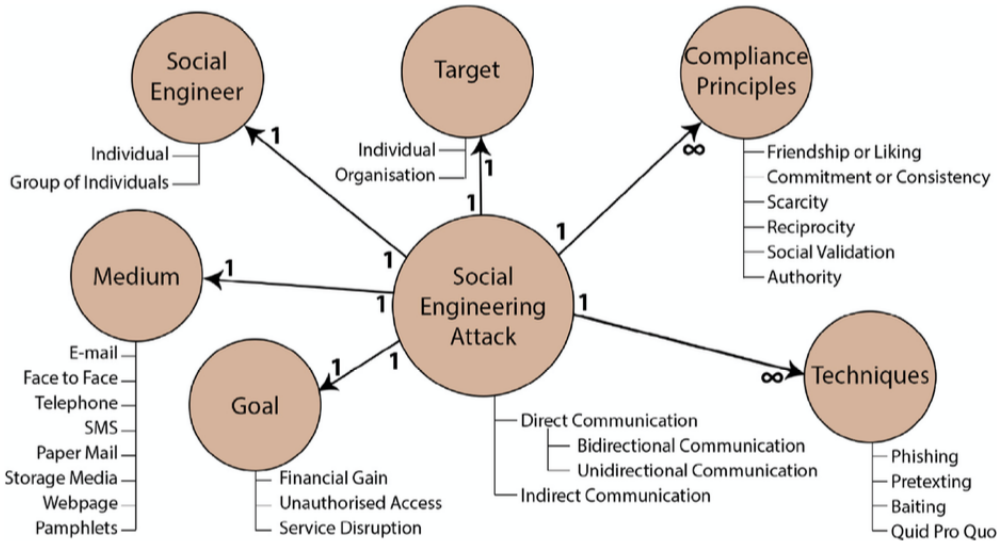

FIGURE 3.7: An ontological model of a social engineering attack [42, p. 4]

seen in the initial steps of an attack sequence [24]. Social influencing techniques are widely used in phishing, i.e: curiosity.

- Forged emails and messages that are meant to catch the recipient's attention. In many situations, it piques the victim's curiosity, gives information on a certain issue, and directs them to a specific website for more information [10].
- A SE could include malicious URLs or embedded links to redirect victims to an attacker-controlled domain that hosts exploit codes or could be a clone of legitimate websites with URLs that appear legitimate.
- There might be malicious attachments in the email, e.g., documents that appear to be a regular Microsoft Word file but do contain malware that will be installed once the victim downloads the file.
- Phishing email messages have a subject line that attracts the recipient to believe that the email is sent from a trusted party. Elements such as texts, logos, images, and styles are used on the legitimate website to make it look authentic.
- Phishing campaigns usually target large groups of people to get the most out of the attack.
- Spear-phishing attacks are aimed at particular targets and often have specific purposes with the attack and higher damage potential and success rate than phishing.

3.3.3.2 Pretexting

In a pretexting attack, a fake situation is created to make the target feel obligated to obey the attacker under false premises. In this situation, an attacker creates a persona to impersonate someone, e.g., a person in an important or powerful position to instruct the target. Pretexting can use emails to get in touch with their target or fake numbers.

3.3.3.3 Baiting

In a baiting attack,the adversary "drops" something either physically or online that catches the targets attention. This might be a USB infected with a malicious script, left in a location that is likely to be found by the targeted victims. The result here would be that the victims' curiosity is triggered, leading to the medium getting inserted into a machine, and the script is executed.

3.3.3.4 Quid Pro Quo

The meaning of the term "quid pro quo " is something for something *latin*, which in a social engineering attack involves request for information in exchange for something. [49] has described the following scenario: *"A quid pro quo scenario could involve an attacker calling the main lines of companies pretending to be from the IT department, attempting to reach someone who was having a technical issue. Once the attacker finds a user who requires technical assistance, they would say something along the lines of, "I can fix that for you. I'll just need your login credentials to continue." Simply the attacker would harvest user credentials. This is a common social engineering attack that non-advanced attackers commonly carry out. These attackers do not have any advanced tools at their disposal and do not research the targets."*

3.3.3.5 Water Hole Attack

a water hole attack is a social engineering technique where the attacker seeks to compromise a specific end-user or a group of end-users by creating new websites that would attract them or infecting existing websites familiar to the targets.

3.3.3.6 Tailgating

is an attack technique where the attacker works towards gaining unauthorized access into a secured area physically, e.g., by walking behind a person

who legally has access to this area. The tailgater will put on a persona that will let them into the area. This technique relies heavily on people's innate desire to be helpful or friendly.

3.3.4 Performing a Comprehensive Cyberattack on Critical Infrastructure

We look at how social engineering has been used to succeed in sophisticated cyberattacks. In recent years, many cyberattacks occurred where social engineering techniques were used both in advance of an attack as a prelude and side-by-side with technical hacking. In the following sections, attack analysis' describes real cyberattacks on critical infrastructure, where social engineering has been used to compromise systems. We want to emphasize the importance of focusing on protection mechanisms social engineering in a world with IoT and smart cities, where critical infrastructure is exposed to the Internet through the attacks described below.

3.3.4.1 Stuxnet: Sabotage on Iranian nuclear power station

Stuxnet is a sophisticated worm designed only to target specific Siemens SCADA (Supervisory Control and Data Acquisition) systems. It is the first-ever known malware that targeted a specific vulnerability in Simens SCADA systems and proved that it could attack control systems and inflict physical damage with software. The malware, however, can spread using USB drives and can be specifically crafted to sabotage SCADA systems that control electric grids [40].

It is believed that this cyberweapon was mainly designed to sabotage nuclear enrichment facilities in Natanz, Iran, specifically. In 2007, the control system in the nuclear plant sabotaged the uranium enrichment facilities due to being infected with Stuxnet. Thus, leading to stopping the Iranian nuclear program. There were mainly two attacks at the nuclear plant: The first attack aimed to increase the centrifuges' overpressure, a secret operation where the attackers kept a low profile. The second attack, in 2010, was aimed to increase the centrifuge engines' speed to destroy them. The damaged product became infected in the plant, pretending to be a "man-in-the-middle" attack. Thus, the virus overpowered the operators. Stuxnet destroyed about 1,000 of 6,000 centrifuges at the Natanz nuclear plant [6]. The worm has, in recent years, also spread to other industrial and energy-producing facilities. Due to

the nature of the attack, Stuxnet is attributed to be made by a state-sponsored threat actor.[58] [36].

There are several theories about how Stuxnet infected Iranian nuclear facilities. Figure 3.8 illustrates ways in which the worm reaches the PLCs (Programmable Logic Controllers) that are controlling the centrifuges. PLCs are special-purpose computers used for controlling electronic devices or systems, such as industrial systems. The PLCs are connected to computers that control and monitor them, and typically, neither are connected to the Internet. One strongly emerging theory about the spread is that Stuxnet is that the systems were infected with a USB. Outside contractors working at the plant may have brought the infected flash drives to the control systems in the instance of Natanz. Whether this was done by baiting, tailgating, or other techniques, the conclusion is that the process must have included manipulating people [43].

The worm was very sophisticated and advance, so was the attack. To construct such a worm, significant amount of time and money is involved, as well as knowledge about the systems nuclear enrichment plants, that were kept secret. To still manage to create something that can attack a system a country keeps hidden, is not an easy job. Stuxnet is strongly linked up to be designed by a state-sponsored group.

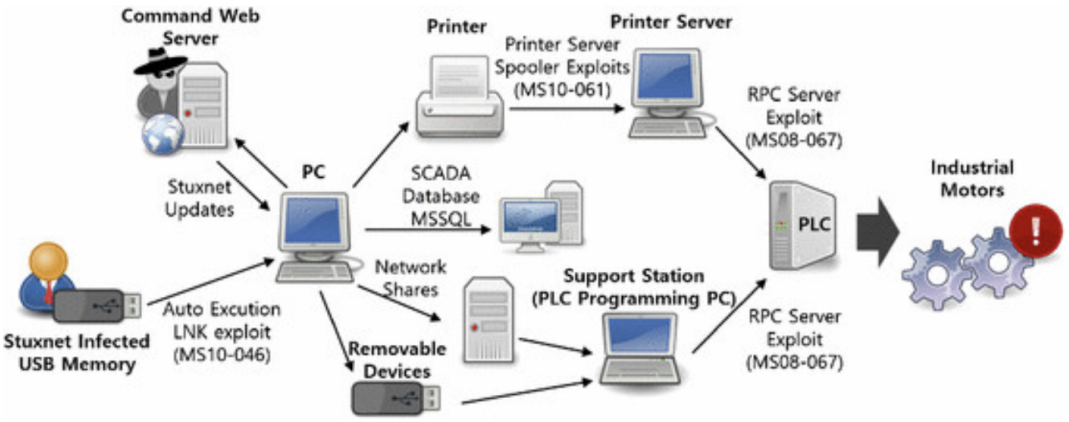

FIGURE 3.8: Stuxnet [51]

3.3.4.2 Cyberattack on The Ukrainian Powergrid

On December 23, 2015, an electricity distribution company (Kyivoblenergo) reported service interruptions to customers. The disruptions were due to a third party and compromise of the company's computers and control systems (SCADA). Later statements indicated that the cyberattack affected additional parts of the distribution network and forced operators to switch to manual operation. The cyberattacks carried out against the companies were well planned, coordinated, and sophisticated. Due to the nature of the attack, it was quickly linked up to be carried out by an APT (Advanced Persistent Threat) national state group.

The attacks consisted of several elements, which involved activation and supported attack segments. The threat actors were remotely connected and engaged in the system. Prior to the attack, the attackers sent targeted emails to specific individuals in the organization. The spear-phishing emails appeared to be from a trusted source but contained malicious attachments. An attack analysis shows that the malware BlackEnergy3 (trojan horse) developed to trigger a denial of service (DDoS) was designed to establish a foothold and use keystroke loggers to perform a credential test. By performing the above steps in advance of the attack, the attackers achieved rights to move further into the system and could tamper with the IT infrastructure. After this, they began to utilize the necessary information and discover the host units. In this way, the threat actors could devise an attacking concept to hijack the SCADA system and then manipulate switches to cause power outages[6][9].

SANS ICS and E-ISAC [9] analysis of this attack explain through cyber kill chain, how social engineering techniques were used to make this attack successful and go into depth about how attacks on critical infrastructure can be carried out and what consequences it can have.

The following is a consolidated list from [9] of the technical components used by the attackers:

1. Spear-phishing to gain access to the business networks of the oblenergos (Regional power distribution entity)
2. Identification of BlackEnergy 3 at each of the impacted oblenergos
3. Theft of credentials from the business networks
4. The use of virtual private networks (VPNs) to enter the ICS network

5. The use of existing remote access tools within the environment or issuing commands directly from a remote station similar to an operator HMI
6. Serial-to-ethernet communications devices impacted at a firmware level
7. The use of a modified KillDisk to erase the master boot record of impacted organization systems as well as the targeted deletion of some logs16
8. Utilizing UPS systems to impact connected load with a scheduled service outage
9. Telephone denial-of-service attack on the call center

3.3.4.3 Hydro Ransomware attack

The ransomware attack on the Norwegian power producer and supplier of aluminum and aluminum products, Norsk Hydro ASA, in 2019 is believed to be a result of social engineering. The malware was delivered three months before the attack when an employee unknowingly opened an infected email from a trusted customer whose network was already compromised. That allowed hackers to enter Hydro's systems and plant the ransomware LockerGoga. Antivirus programs missed the sample of LockerGoga supposedly because the ransomware had a valid digital signature. Once it gained access to the system, it was able to perform the following stages:

- Change users' passwords as well as try to log them out,
- Denying access to the systems,
- Encrypt stored files of specific types in all the accessible machines, meaning desktops, laptops, and servers that are connected to the network

Information through several sources indicates that the LockerGoga virus seems to be targeted towards production industries as at least five attacks are known to happen during 2019. The attackers disrupted services and gained money[33].

Chapter 4

Design and Implementation

In this chapter we present scenarios based on selected attack techniques we conveyed through Chapter 3. Exploring the range of alternative scenarios allow us identify potential adversaries, risks and impact of the attacks. We provide a illustrative description of the attack through figures. In each of the scenario subsections, we examine the nature of the attack and provide an analysis discussing the adversary involved and implications of the attack. We end the chapter with a discussion about the attacks and their implications.

4.1 Goal

In this chapter the main goal is to

1. Identify possible threat agents to the energy sector with focus on Advanced Metering Infrastructure.
2. Create different scenarios based on attacks that exploit human behaviour and cellular network communication.
3. Analyze the scenarios and the potential impacts of the attacks, and outline these through an analysis

4.2 Identifying Threat agents to Advanced Metering Infrastructure

In order to work with the threat agents in our scenarios, we have analyzed the adversaries to gain knowledge about different threat actors that are out there before narrowing them down to threat actors that are relevant to our

scenarios. With the aim of understanding, analyze and responding to cyberattacks, it is crucial to identify threat agents, their motivation, and their capacity [61].

In our study, we present seven threat agents. Threats emerge from a group of threat agents, and it is considered essential for Smart Grid assets owners and users to know the threats that emerge from which threat agent groups. This information is significant in deciding on the risks that should be mitigated: Threat agent groups indicate the determination behind launched attacks and capability level. Given the importance of the Smart Grids and the potential impact of attacks, Smart Grid asset owners will need to consider which protection might be appropriate to avoid exposure to attacks from a specific type of threat agent. The threat agents considered within this document are as follows:

- **Corporations:** This kind of threat refers to companies (corporations, organizations, enterprises) that adopt and or are engaged in offensive tactics. In this context, corporations are considered hostile threat agents, and their motivation is to build a competitive advantage over competitors, who also make up their primary target. Depending on their size and sector, corporations usually possess significant capabilities, ranging from technology to human engineering intelligence, especially in their area of expertise.

- **Cybercriminals:** Cybercriminals are hostile by nature. Moreover, their motivation is usually financial gain, and their skill level is, nowadays, relatively high. Cybercriminals can be part of a local group or organized on a national or international level. It should be taken as given that a certain degree of networking between cybercriminals is being maintained.

- **Employees:** also known as the *"insider threat"*. This category refers to the staff, contractors, operational staff, or security guards of a company. They can have insider access to the company's resources, and they are considered both non-hostile threat agents (i.e., distracted employees) and hostile ones (i.e., disgruntled employees). This kind of threat agent possesses a significant amount of knowledge that allows them to place effective attacks against their organization's assets.

- **Hacktivists:** Politically and socially motivated individuals who use computer systems to protest and promote their cause categorizes as

hacktivists. Hackactivism is a combination of hacking and activism. The hackers can vandalize and cause havoc, targetting websites (deface websites to convey a message). Moreover, they are usually targeting high-profile websites, corporations, intelligence agencies, and military institutions.

- **Nation-states:** In the past few years, this group has become a prominent threat agent in the digital domain due to the deployment of sophisticated attacks considered cyber weapons. Nation-states can have offensive cyber capabilities and use them against their targets. From the sophistication of a process or executable, it can be confirmed that nation-states have a plethora of resources and a high level of skills and expertise. Attacks carried out by this group are often linked to intelligence activities, such as digital espionage, creating disruptions and sabotage in critical infrastructure, or negatively affecting a nation through the cyber domain.

  An advanced persistent threat (APT) is a broad term used to describe an attack campaign where the cyber threat actor(s) establishes an unauthorized, long-term presence on a network and laterally moves further into the systems. The APT term is usually applied to nation-state actors who carry out cyberattacks on behalf of nations. There are usually teams of skilled IT personnel (from an IT company or experienced cybercriminals) involved and funded by the government. Their targets are carefully chosen and investigated and are typically as large enterprises or governmental networks, and the attacks are used as cyber warfare weapons.

- **Natural disasters:** Natural disasters are also threat agents, and organizations are influenced by them, as they can cause potential physical damage. Natural disasters include lightning, fires, floods, earthquakes, windstorms, and many more. Although not a human threat agent, natural disasters are considered as such, as they can cause severe physical damage and impact the availability of information systems.

- **Terrorists:** Terrorists have expanded their activities and also engage in cyber-attacks. Their motivation can be political or religious, and their capability varies from low to high. Preferred targets of cyber terrorists are mostly critical infrastructures (e.g., public health, energy production, telecommunication), as their failures cause severe impact on

society and government. It has to be noted that in the public material analyses, the profile of cyber terrorists still seems to be blurry.

- **Cyber fighters:** an emerging phenomenon is motivated patriotic groups of citizens to launch cyber-attacks potentially. Such groups might have strong feelings when their political, national, or religious values seem to be threatened by another group and can launch cyber-attacks. One can argue that such groups are exceptional cases (maybe an evolution or yet another instance) of hacktivism. To an extent, such groups may be supporters of totalitarian regimes and, rightly or wrongly, act on behalf of their supporting parties (i.e., governments) by contributing to national activities in the cyber-space. Their activities may include conflicts with other groups (i.e., hacktivists).

Extracting threat agents towards the energy sector

Based on these short threat agent profiles, we have mapped which threat group is most relevant to be assigned to our scenarios. The following questions have helped us narrow down the possibilities of attackers:

- Who has the motive for attacking a target in the energy sector?
- Who has targeted this sector earlier?
- Who has the resources and capacity to attack a target in the power sector?
- Who has the capacity to design an attack/malware/virus or find zero-days for systems?

Cyberattacks targeted towards industrial control systems are usually politically motivated terrorism to disrupt a nation's critical infrastructure or are a part of an industrial cyber-espionage operation or cybercampaign for financial gains. We chose three different actors to include in our study based on our research, the news picture, and the questions above. We think these threat agents have an interest in disrupting services provided by the energy sector:

- State sponsored nation threat APT
- Cybercriminals
- Hackativists

4.3 Application on AMI: social engineering

4.3.1 Scenarios of social engineering

4.3.1.1 Scenario 1: phishing

Assumptions: the threat actors have taken control over the utility's cloud infrastructure and have gained extensive system knowledge. They have created a (fictive) ransomware called PowerLocker. If executed, the Powerlocker locks the mobile screen and can send random commands into the smart meter application that will cause disruption in the smart appliances in a household. The ransomware works on Android and iOS.

Potential threat actor: cybercriminals

Goal: financial gain

Target: smart meter interface

Medium: e-mail, webpage

Technique: phishing

Attack scenario: Shinra Electric Power Ltd. uses its cloud platform to deliver updates, new content, and messages from the smart meter company to the smart meter application at the consumer's side. The application is installed on Android and iOS devices, and users are able to control their smart appliances through this application.

In this scenario, the threat actor group Gator Gang, has established a foothold in Shinra Electric Power Ltd's cloud infrastructure. The attackers use the cloud system to carry out cyberattacks.

The Gator Gang has been in the systems for quite some while, and has access to critical secret documents about the system and data on their customers. The attackers have previously gained knowledge about the different customers and are informed that many well-off people are customers of Shinra Electric Power Ltd. The hackers have been tasked with carrying out several attacks from this platform. Their main mission, for now, is to construct a phishing SMS leveraging their ransomware called PowerLocker to the company's customers:

Subject: *"System reset"*
Dear customer
As a result of a system patch, you have to reset your smart meter. Please visit www.resettemp.zy as soon as possible to reset the system. We apologize for any inconvenience caused by the latest update.
Best regards, Shinra Electric Power Ltd.

———

www.resettemp.zy is not linked up with the smart meter application but is a website hosted by Gator Gang. When clicking on the link, the consumer gets a pop-up message saying *"Smart meter was successfully reset"*. Few seconds after the pop-up message, the following message pops up:

———

Your telephone is now locked, and all your files on the device are encrypted. Pay the the amount of $10 00 in BAD[1] to address: 1BvBMSEYstWetqTFn5Au. The payment can be made at www.gatorGang.onion.zy
We have access to all your IoT appliances and are able to control them. If the amount is not paid right away, we will increase the heat of the devices. PS: restarting the telephone will not remove the locker.
We guarantee you that once the amount is paid, you will receive a decryption key immediately. If you already have received the key, enter it here:

Gator Gang

———

If the amount is not paid, random commands are sent to the smart phone application. The random commands result in the washing machine being switched on, the heating system is switched on fully, households being blacked out.

[1] Fictive crypto value

Illustrative examples:

The figure 4.1 describes the scenario: how the attackers carry out the attack. Starting with compromising the TTP *(Shinra Electric Power Ltd)* and the customer with the smart meter, receiving the malicious link on SMS.

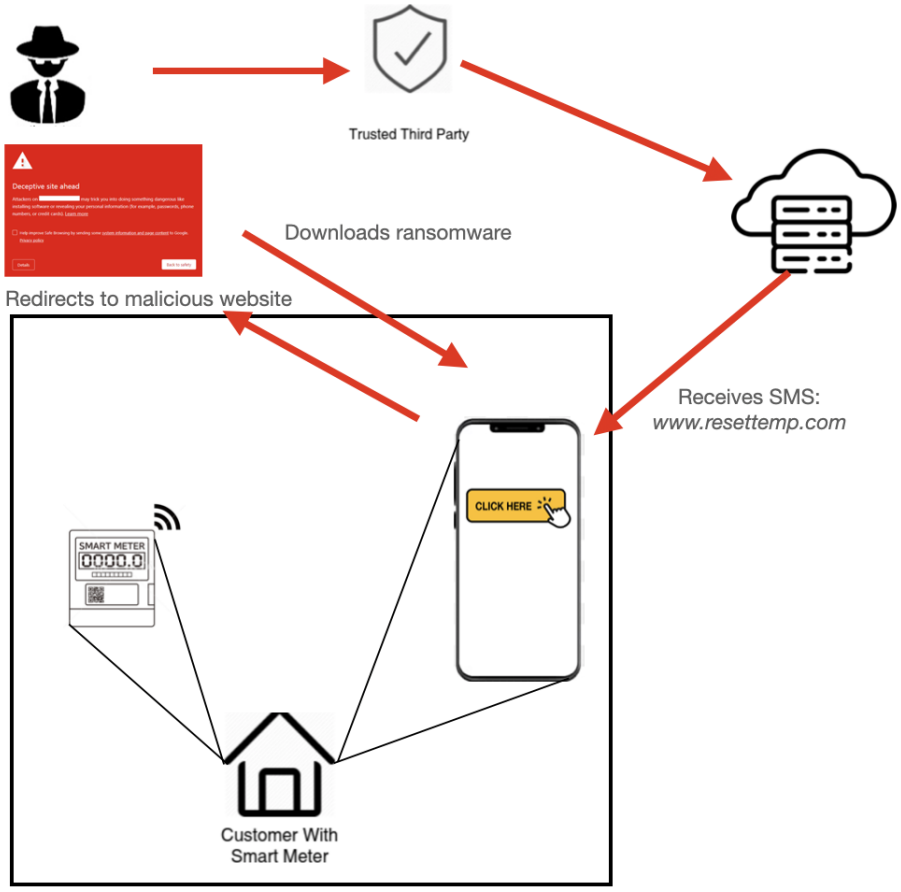

FIGURE 4.1: Scenario 1: Phishing

Analysis and implications:[2].

The attack is socio-technical in character, combining social and technological approaches. The actor impersonates the company with authority in order to deceive the victim into believing what they say. Pretexting, phishing, and pharming are all used in the attack.

Prior to the attack, Gator Gang performed preparations, including reconnaissance on customers and the systems. Their ultimate goal is to make money. They know that their victims are wealthy individuals and that targeting them might result in financial benefit.

[2]This scenario is based on the same technique as the Hydro attack in 3.3.4.3, where the attackers had established a foothold in the systems of a customer of Hydro

This strategy mainly relies on an attacker constructing a believable and compelling situation, story, and persona to trick individuals and companies into giving sensitive information or following instructions. Pretending to be Shinra Electric Power Ltd is an efficient method of pretexting that will result in many individuals accepting their orders. In this scenario, pretexting and SMS-phishing are combined. The attackers deceive the victims into clicking on a malicious link that will redirect the consumer to a fake website (pharming attack). An executable is downloaded and executed on the victims' phone once the victim clicks on the link. This fictive ransomware has two properties: lock the screen, and send random commands to the smart meter app affecting the appliances that are registered within this app. Even though cybercriminals do not want to harm people or put their lives in danger intentionally, the impacts of sending random commands to the smart meter application might have disastrous consequences in the scenario described. Considering a worst-case scenario: a person's breathing equipment fails as a result of this attack.

The method of payment that the threat actors are asking for is well-known. Cryptocurrencies are adopted as a payment mechanism in both traditional and cybercrime to retain a certain level of anonymity. A crypto wallet does not require any personally identifying information, unlike a bank account. Unless discovered through other methods, the identity of the crypto wallet address holder stays hidden.

4.3.1.2 Scenario 2: physical access to the smart meters

Assumptions: threat actor has knowledge about system HW and SW, smart meters are installed in bundles in a room in the basement of the apartment complex

Threat actor: hacktivist

Goal: get physical access to the smart meter

Target: smart meter device

Medium: physical appearance

Technique: tailgating

Attack scenario: our scenario revolves around an apartment complex with smart meters installed in a basement room that is accessible to everyone in the building. Everyone who owns a car has to go via the basement to get to

the parking garage. As a result, there is are many people on their way to the basement in the morning.

Eve is a member of the national stop-increasing- the electricity-prices-party- and is very motivated to do anything to get back on the power companies increasing the power consumption prices. On behalf of the party, Eve will be sabotaging a bundle of smart meters. Information, the party, has collected indicates that smart meters are installed in the basement in the apartment complex at the address Grimmauld Place 12. Eve dresses nicely and arrives at the address at 8:00 a.m. She waits for a resident to enter the basement. Eve says to them: *"Thank God you came around, I forgot my keys upstairs. Running late for a meeting and I would never have been able to go back and get my keys"*. The resident opens up the door to the smart meter, and Eve follows after. Eve has now performed a tailgating attack and has full access to the smart meters.

Illustrative examples: figure 4.2 describes the tailgating attack, where an adversary follows after a person with access.

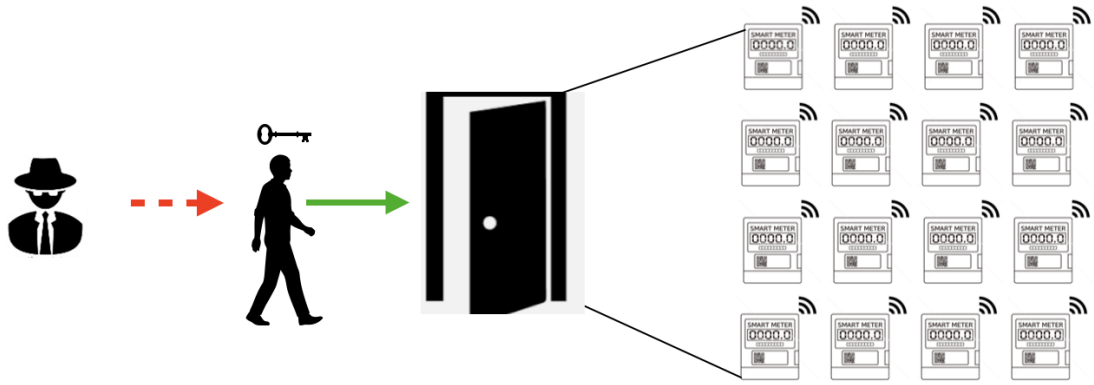

FIGURE 4.2: Scenario 2: Tailgating

Analysis and implications: this is a low-level attack that needs very little time and financial resources to perform. In comparison to the other threat actor groups studied in this thesis, hacktivists have fewer financial resources. They frequently rely on off-the-shelf components or scripts obtained online (i.e., GitHub, GitLab, Darkweb). As a result, we opted to look at the attack through the eyes of a hacktivist: it is a low-cost and straightforward technique to get access to the device, no special equipment is necessary, and accessing the smart meters opens the door to causing AMI services disruptions.

Elements such as the threat actor being well dressed and meeting at 8:00 a.m. could lead one to believe that the person is going to work, conference or meeting at the stated early hour and are well-dressed. Another important factor to consider is that many people are unfamiliar with the notion of a smart meter. Many of them have no clue where they are, so the idea of protecting it does not occur to them. Only these two criteria, if used correctly, can raise the chances of a successful social engineering attack. Most people feel it is typical politeness to hold a door or open a door for someone. Eve has to take advantage of this human weakness to get physical access to the target and get beyond the initial physical barrier.

Using tailgating as an initial vector provides the attacker with infinite opportunity space to launch further attacks. The consequences of such attacks are numerous, but the most important is the freedom to carry out other attacks: We presume that an attacker can read and write the contents of a smart meter's memory. As a result, an attacker can insert malicious code into a smart meter's vacant memory space. In addition, the attacker has the ability to listen in on any data transferred through AMI networks, change specific data, and send any data to a selected destination (e.g., a smart meter or a verifier). On the other hand, an attacker is unlikely to replace a smart meter's hardware specification. Examples are modifying the smart meter's BIOS, adding memory, changing memory access time, and raising clock frequency. Through physical access, the threat actor gets the opportunity to gain insight into smart meter components (such as the GPS tag and messing with it). This means that an actor can acquire knowledge about hardware, practice reverse engineering techniques to attack the meter further, find zero-days, or, i.e., sell techniques and system information in the Darkweb. The attacker could also install a rouge meter in the network. This type of attack could compromise a target's privacy in different ways: check the meter readings to see if a specific target is a home, when they are home, and when they have high consumption. Such information could be used to commit a robbery, for instance. Given the goal of our hacker Eve, she would most likely not perform an attack that would cause widespread harm to the system. This threat group regularly engages in vandalism, small-scale sabotage, and other means of undermining to get their message out without hurting anybody or creating widespread system damage. Considering these points, Eve would most likely cause physical harm to the system, which would have limited impact on the grid, but may affect the local HAN and billing/consumption calculations. This can increase the cost of utilities considering that the billing

information is incorrect and that they have to spend costs on reinstalling the meters.

4.4 Application on AMI: cellular network attacks

4.4.1 Scenarios of cellular network attacks

4.4.1.1 Scenario 1: NAN-sniffing

Assumptions: the threat actors have found a backdoor in the data concentrator server - a zero-day vulnerability

Potential threat actor: state-sponsored nation threat APT

Goal: monitor the traffic passing through the node, in a passive manner

Target: data collector

Medium: NAN-network

Technique: exploit a zero-day in the data concentrator

Attack scenario: A group of well-organized hackers has been researching a specific type of concentrator server for quite some time. They have figured out the admin password and username, which they use to access the server. To ensure a high level of anonymity, they are using TOR and VPN before logging onto the target server. The threat actor is able to sniff traffic that passes through because they are on the node. The threat actor has not only logged on to one concentrator but also many others in different NANs. In addition to the NAN-sniffing, the group leaves a maliciously customized script. If executed, the script sends loads of data packets to the smart meters in HAN and the WAN.

Illustrative examples: The illustration shows the art of the attack. A group of hackers uses TOR and VPN prior to logging on to the server. The script shown in the figure triggers the red striped arrows.

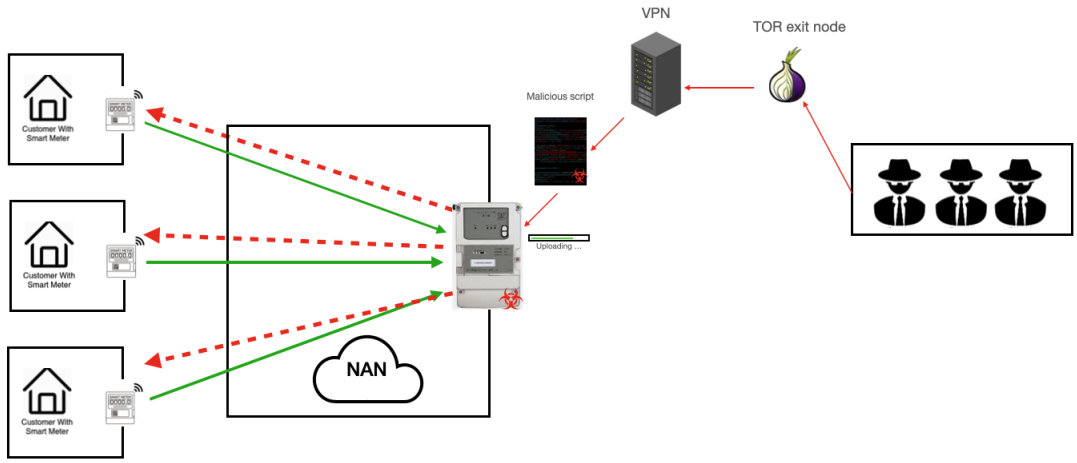

FIGURE 4.3: Scenario 2: Packet sniffing

Analysis and implications: We attribute this attack to a nation-state threat APT because of its advanced nature: the scenario outlines a threat actor with high operational security (opsec) who uses TOR and VPN to disguise their source IP and has admin access to the data concentrator. Furthermore, doing zero-day research involves time and money, which not every threat actor has. APTs that pose a national security concern are funded and supported by the government in every way and have unrestricted access to resources. Another common APT strategy is to upload the scripts to the server and use the server as a command and control (C2) unit. The primary purpose of this attack is to carry out a packet sniffing attack. In the long run, however, the attacker may do a lot more merely by being on this node, both in terms of passive attacks like spying, sniffing, and other MITM attacks, as well as active attacks like launching a DDoS attack. A DDoS attack can involve sending large data packets to the meters or compromising more of these concentrators, and forming a botnet. Compromising the concentrator can also affect the WAN side: hackers could modify the data transferred to the HES. The packets could even be infected with malware and transferred to the HES, further damaging MDBS or the HES system.

4.4.1.2 Scenario 2: DDoS

Assumptions: The smart meter is infected with a (fictive) malicious botnet malware called Zad

Potential threat actor: nation threat actor, cyber criminal

Goal: steal information, monetary gain, disrupt services

Target: NAN-network, smart meters and the concentrator

Medium: Smart meter

Technique: DDoS attacks using a botnet

Attack scenario: A group of attackers have infected several smart meters in various NAN networks. They have infected the meter with a specific botnet malware called Zad. This is a malware specifically designed to compromise meters.

Illustrative examples:

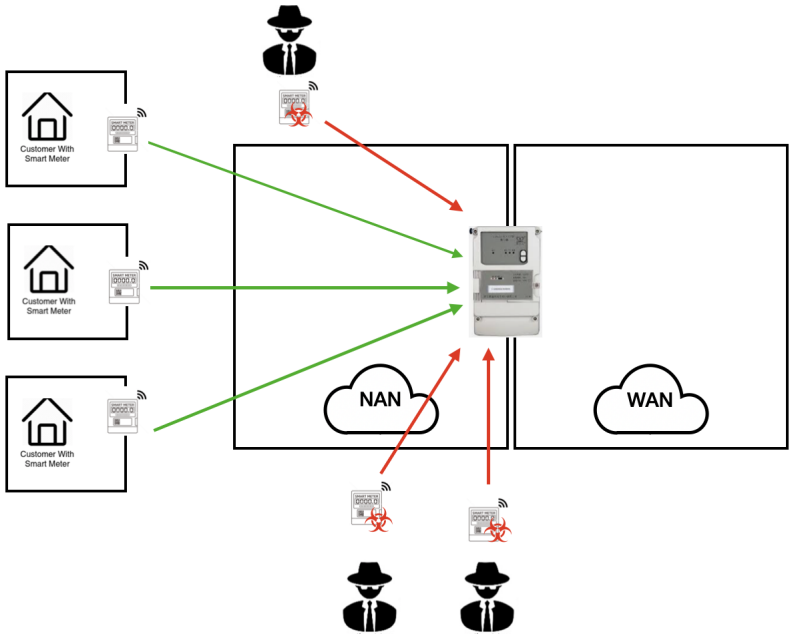

FIGURE 4.4: Scenario 2: Smart meter botnet

Analysis and implication: The attackers have constructed a botnet of rogue smart meters in this operation. They infected the meters with malware that was specifically designed for this purpose. In addition, such devices facilitate lateral propagation of malware, introducing more infected devices to participate in the botnet. The consequences of such an attack might be manifold, depending on who is responsible for the attack. We take a deeper look at two groups of hackers we believe could have been involved in such an attack.

Looking at this attack from the perspective of a nation-threat, a botnet like this might be utilized for various purposes. One of the points we want to highlight is that a botnet like this may be used for espionage purposes,

both in terms of gathering information about individuals and industrial espionage, in which the actor gains system and program knowledge. A more active move, in wartime, for example, would be to use this botnet to carry out DDoS attacks to destroy systems or create disruptions to affect the Smart Grid.

A cybercriminal would not operate in the same way. As we have seen before, cybercriminals are generally motivated by financial gain. In this situation, the threat actor might threaten the utility by claiming that they have taken over the network and would damage if they do not receive the amount they asked for. Selling vulnerabilities, botnets, and malware on the dark web to other parties who may benefit more by actively targeting the NAN network. Cybercriminals, for example, may sell this to a nation-state threat for a certain amount of money.

4.5 Discussion, weaknesses and limitations

4.5.1 Discussion

Both the human aspect and the cellular networks impact the AMI system in the energy sector but in two distinct ways. While the cellular network connects the various AMI components and allows data flow between them, the human role resides on the HAN and WAN sides, respectively as a smart meter user and a utility employee. The human factor and cellular communication networks have a substantial influence on the infrastructure's physical and cybersecurity. If these vectors are hacked, the entire system is threatened.

Cyberattacks are becoming increasingly widespread in businesses and governments throughout the world. Public utilities, which are also vital to daily living, are among the most vulnerable to cyberattacks. Despite the fact that the electric grid is the most necessary public utility in terms of daily activities, threat actors seek to damage it. The consequences of a large-scale grid attack might be severe and far-reaching.

The scenarios we propose in this thesis highlight how a threat actor might exploit vulnerabilities in AMI through wireless network attacks and social engineering approaches. In order to be able to define best practices in terms of mitigation techniques and security measurements, it is necessary to consider the assets that are being administered and threat actors that may be

interested in compromising these AMI assets. It is necessary to consider the effects of a possible breach on these assets if they are compromised.

Having IoT devices in the AMI without sufficient security measurements leads to many vulnerabilities such as targeted code injection, MiTM attacks, spoofing, hijacking, and weaponizing various components of AMI in order to leverage these for further attacks. Because there are large amounts of data in the Smart Grid, malware might be easy to hide, and IoT devices could come preloaded with malware. We have not looked at the latter, although it is possible that vulnerabilities and infections were deliberately introduced (i.e, by nation threat actors in order to spy).

Our scenarios highlight that there is much money to be made (for cybercriminals) or loss of income (especially for utilities) if AMI were to be attacked. In addition to this, attacks can be used to paralyze a nation if the attack is widespread enough to affect the Smart Grid. Suppose a country's power is cut out. In that case, the emergency network may not function, individuals who rely on breathing machines or other machinery for survival may not be able to function, emergency units may not function. In other words, critical social functions will be disrupted.

We have used three different hacker groups that we consider the energy sector to be attractive for when carrying out an attack. Modern cyberattacks against AMI have targeted nation threat APTs, who design complex and sophisticated network attacks. Experienced hackers get unauthorized access to the AMI network using zero-day malware and remain undetected for a long time. APTs are known to attack high-value targets such as other nations, critical infrastructure, and large corporations. The ultimate goal is to collect information, usually over a long period, quietly and then use it during times of conflict and war. AMI is an excellent target for their target portfolio since they can conduct cyber-espionage as well as active attacks against AMI that can disrupt the whole Smart Grid. Hacking activists can inflict damage to convey a message or to create dedication around an issue that is important to them. Cybercriminals attack for monetary gain through ransomware or selling vulnerabilities/botnets/technologies.

Our scenarios and the real-life examples presented in Chapter 3 on social engineering outlines that technology and cybersecurity measurements are not enough to keep assets secure. The human element must be considered: the employees and the users are the first line of defense against a cyberattack, but as our research shows, human is also the weakest link. In 4.3.1.1 the

social engineering factor is quite strong and it is difficult for the customer to avoid clicking on the link as it seems to be from the company. One important thing to note here though is that the company only sends out updates and messages through its application, not via SMS (as indicated in). Another thing one can do is assess the credibility of the link.

An important thing to remember from Chapter 3 is the various network technologies implemented in AMI. To limit ourselves, we have not covered the vulnerabilities on the HAN side. However, various cellular network technologies make AMI vulnerable in different ways. Different bandwidth and capacity requirements for different applications on the devices and components are why many network technologies, channels, and protocols exist. However, various network technologies offer one of the most significant challenges: providing security on every network path.

Both network attacks and social engineering can have catastrophic implications if applied on AMI. The scenarios illustrate key aspects of the threat actor, their purpose, and vulnerabilities in AMI, and their consequences once they have been exploited. We already know from Chapter 3 that both human and wireless networks are vulnerable to hacking in a variety of ways. We were able to design scenarios based on prior attacks and attacks now occurring on the IoT. The scenarios are necessary to demonstrate what may occur, how it can occur, and who can cause it to occur. A lot of our discussion and analysis is provided within the "Analysis and implication" parts in each scenario.

4.5.2 Weaknesses and limitations

The knowledge gathered from the literature research (attack tactics) is not applied to the AMI in reality, which is the study's main weakness. We have created scenarios by combining data and information conducted through the literature review. These scenarios are instead a description of the possible outcome of attacks in the future. As a result, we do not have a proper outcome and cannot validate or contradict the implications of the attacks described in the scenarios.

Social engineering, wireless cyberattacks, smart grid security, AMI vulnerabilities, and cellular network technologies have been the subject of several research studies and are quite well covered in different studies. Looking at these topics together and linking these to the interests of different actors has

been challenging due to the lack of previous references and research. Another thing that is important to state is that the problem and goals of the thesis are quite widespread, we highlight many topics. For future work, it is preferable to narrow down the topics, e.g. study one component of AMI at the time, rather than the whole infrastructure.

We have made certain choices regarding presenting the different attack techniques. We have limited ourselves to briefly discussing the main category of the attack because the attacks we describe in the thesis have several subcategories. Botnets, for example, may be used to carry out a variety of attacks, such as spamming, passive espionage, and DDoS attacks. When it comes to DDoS from a botnet, there is a wide range of options. It all depends on which layer in the network the attack is launched from, whether from the application layer or the network layer. HTTP flooding Attacks, DNS amplification attacks, session initiation protocol attacks (SIP) flooding is only one of the various types of attacks. We had to limit ourselves in terms of what we present in the thesis and describe the primary categories of the attacks, which may give an inaccurate image of the outcome of the scenarios (whether or not the attack is successful). Consequently, to obtain a correct result, it is crucial to validate in practice with that correct subcategory of the attack.

Chapter 5

Conclusion and Further Work

We are heading into the era of the Internet of Things(IoT), and the number of interconnected devices is increasing. Critical infrastructure in the health, finance, transportation, and energy sectors are being transformed with IoT technologies. Parallel to this, the threat landscape with new vulnerabilities is expanding, which is of major interest to threat actors. Cyber attacks on critical infrastructure are essential to learning as the attacks are increasing when devices are exposed to the Internet.

In recent years, industrial systems have adopted more standard technologies. As a result of the implementation of such technologies, critical systems become more vulnerable to physical and digital attacks. Cyber attacks of various types and magnitude have been on the rise, targeted at the energy sector, specifically at Smart Grid infrastructures. The Smart Grid is sought after even by state-sponsored threat actors and in an intelligence context. A successful attack on the grid could have significant impacts, including grid shutdown, cascading failures, damage to the infrastructure, and potential harm to people. Smart grid infrastructures are critical in nature; they enable operations for residential, commercial, industrial, and government users across critical infrastructure such as water, communication, banking, transportation, manufacturing, and more. The compromise of these operations introduces threats, which span from economic to public safety.

5.1 Conclusion

This thesis studied broad topics within the digital domain that are highly relevant today regarding growing cyberattacks on critical infrastructure, and more specifically attacks on the energy sector. The focus of this thesis has been to provide theoretical insights into ways of compromising the wireless

cellular communication network as well as the human factor in technology, in order to perform cyberattacks on advanced metering infrastructure. Attacks on AMI could affect the whole grid.

We proposed the following questions in the introduction: *What are the attack possibilities on the Advanced Meter Infrastructure?*; and *What possibilities are available to a determined attacker to apply known social engineering attacks to compromise AMI and its components in particular?*

We have done a thorough assessment of the components of AMI, the risks and vulnerabilities related to them. We learned from the research that the main components provide a broad vulnerability surface that may be exploited by a variety of attackers performing different attack techniques. The attack surface is as follows: physical and cyberattacks can be used against the smart meter. We discovered that many smart meters in Oslo are not properly secured as a result of our research. The meters are installed in bundles in shared basements accessible to anybody with a key, which inspired our 4.3.1.2. Like smart meters, data concentrators are vulnerable to both cyber and physical attacks. Because the concentrator servers may run on a Linux-based operating system, which is well-known in the hacking community, they can be easily hacked if not properly secured. The headend system that contains meter data associated with consumers resides at the DSO. This is prone to inside attacks and can also be exposed to network attacks if the WAN network happens to be compromised.

We have studied how wireless cellular network attacks and attacks compromising human behavior can be applied to AMI. The attacks mentioned in this thesis are not unique or exclusive to only AMI. However, they are highly relevant to a wide range of technologies adopted in the energy sector and other sectors that implement technologies exposed to the Internet.

In the recent years, the energy sector has experienced a significant change, and with this change follows an expanded threat landscape that is vulnerable to many different types of attacks. Smart Grid and its essentials are highly vulnerable due to IoT for many different types of adversaries. We have used three threat groups that we consider the energy sector attractive for when carrying out an attack. Our scenarios highlight that there is much money to be made (for cybercriminals) or loss of income (especially for utilities) if AMI were to be attacked. In addition to this, attacks can be used to paralyze a nation if the attack is widespread enough to affect the Smart Grid. Suppose a country's power is cut out. In that case, the emergency network may not

function, individuals who rely on breathing machines or other machinery for survival may not be able to function, emergency units may not function. In other words, critical social functions will be disrupted. Hence, the need for protecting IoT in critical infrastructure is equivalent to protecting national security. Additionally, some attacks may seek to utilize AMI as a launching point for other Internet attacks because of the vast number of devices, their ability to initiate many-pronged attacks, and even their ability to hide malicious or criminal data through the dispersion of many nodes. In order to prepare a best practice for those who manage AMI and its values, the threat landscape, attack techniques, entry points, and, not least, the profiles of the various actors must be conveyed to them.

One main goal of this thesis has been to highlight that the most widespread types of cyberattacks, namely social engineering and wireless network attacks, can be applied to AMI. We explored the AMI threat landscape through our scenarios and exploited the vulnerabilities that exist in the different components of the infrastructure using social engineering techniques and network attacks. The techniques mentioned above are real and can result in industrial espionage, cyber-espionage, loss of values, money, and confidential information. The worst-case scenario is that life and health are put in danger. Through the scenarios and the implications of the attacks presented, we conclude that human involvement in this system and devices in AMI being exposed to the Internet do form serious risks.

Even though aspects of our research are described in a strategic manner without going in-depth of the technical views on technologies, protocols, and attacks on a technical level, we believe that presenting the strategic aspect is essential for those involved and affected by cyberattacks.

5.2 Suggestions to future work

We have only been able to present the theoretical aspects of the threat landscape of AMI. Our study describes a few attack methodologies in the categories of human hacking and cellular network hacking, scenarios of how an attack is carried out, and the potential implications of such attacks. The research of this thesis would benefit from further work on the following lines:

- Further work on this topic from a technical aspect should be performed in order to confirm or disprove the scenarios given in this thesis. Ideal would be to exploit the described vulnerabilities using malware and

other techniques in a test lab. In addition, there is a need to get hands-on with the AMI system, and reverse the system to disclose unknown vulnerabilities or confirm the already existing vulnerabilities and exploit these with malicious scripts and executable, or just simply tamper with the components.

- Most sophisticated attacks today are carried out by highly skilled threat actors that use social engineering techniques as initial vectors in their attacks. These attacks raise major concerns, and research on human psychology is required.
- In the long term perspective, it is desirable to look at mitigation techniques and technical measurements within cellular communication and the human psychological factors. Despite the fact that we have shed light on some existing vulnerabilities in AMI, we have not developed a best practice to mitigate the vulnerability surface. There is an urgent need to develop a best practice with the industry to apply technology most securely with physical and technical countermeasures.
- We have not proposed any recommendations in terms of security measurements or best practice. In order to propose recommendations, it is necessary to test the scenarios, and analyze the results. This could also be part of future works on this topic.

Bibliography

[1] K Aarika et al. "Perception layer security in the internet of things". In: *Procedia Computer Science* 175 (2020), pp. 591–596.

[2] Muhammad Daniel Hafiz Abdullah et al. "Attacks, Vulnerabilities and Security Requirements in Smart Metering Networks." In: *KSII Transactions on Internet & Information Systems* 9.4 (2015).

[3] Fadi Aloul et al. "Smart grid security: Threats, vulnerabilities and solutions". In: *International Journal of Smart Grid and Clean Energy* 1.1 (2012), pp. 1–6.

[4] Masood Aslam et al. "Smart Grid Communication Infrastructure, Automation Technologies and Recent Trends". In: *American Journal of Electrical Power and Energy Systems* 7.3 (2018), pp. 25–32.

[5] Satin Asri and Bernardi Pranggono. "Impact of distributed denial-of-service attack on advanced metering infrastructure". In: *Wireless Personal Communications* 83.3 (2015), pp. 2211–2223.

[6] Namrah Azam. "Informasjonssikkerhetstilstanden i energiforsyningen". In: *Norges vassdrags-og energidirektorat, Oslo* (2017).

[7] D Bian et al. "Analysis of communication schemes for Advanced Metering Infrastructure (AMI)". In: *2014 IEEE PES General Meeting | Conference & Exposition*. IEEE. 2014, pp. 1–5.

[8] Stuart Borlase. *Smart grids: infrastructure, technology, and solutions*. CRC press, 2012.

[9] Defense Use Case. "Analysis of the cyber attack on the Ukrainian power grid". In: *Electricity Information Sharing and Analysis Center (E-ISAC)* 388 (2016).

[10] Robert B. Cialdini. *Influence: the psychology of persuasion: Robert B. Cialdini*. Collins, 2007.

[11] Frances M Cleveland. "Cyber security issues for advanced metering infrastructure (AMI)". In: *2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*. IEEE. 2008, pp. 1–5.

[12] Christian Dänekas et al. "Towards a model-driven-architecture process for smart grid projects". In: *Digital enterprise design & management*. Springer, 2014, pp. 47–58.

[13] Soma Shekara Sreenadh Reddy Depuru et al. "Smart meters for power grid—Challenges, issues, advantages and status". In: *2011 IEEE/PES Power Systems Conference and Exposition*. IEEE. 2011, pp. 1–7.

[14] Moustafa Eissa. *Smart Metering Technology and Services: Inspirations for Energy Utilities*. BoD–Books on Demand, 2016.

[15] Zakaria El Mrabet et al. "Cyber-security in smart grid: Survey and challenges". In: *Computers & Electrical Engineering* 67 (2018), pp. 469–482.

[16] U.S. Department of Energy. *What Is the Smart Grid*. Youtube. URL: https://www.youtube.com/watch?v=JwRTpWZReJk.

[17] Patrick Engebretson. *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*. 1st. Syngress Publishing, 2011. ISBN: 9781597496551.

[18] Xi Fang et al. "Smart grid—The new and improved power grid: A survey". In: *IEEE communications surveys & tutorials* 14.4 (2012), pp. 944–980.

[19] *GPS Receivers*. 2011. URL: https://gssc.esa.int/navipedia/index.php/GPS_Receivers.

[20] Paul E. Green. "The future of fiber-optic computer networks". In: *Computer* 24.9 (1991), pp. 78–87.

[21] V Cagri Gungor et al. "A survey on smart grid potential applications and communication requirements". In: *IEEE Transactions on industrial informatics* 9.1 (2013), pp. 28–42.

[22] Vehbi C Gungor et al. "Smart grid technologies: Communication technologies and standards". In: *IEEE transactions on Industrial informatics* 7.4 (2011), pp. 529–539.

[23] Aaron Hansen, Jason Staggs, and Sujeet Shenoi. "Security analysis of an advanced metering infrastructure". In: *International Journal of Critical Infrastructure Protection* 18 (2017), pp. 3–19.

[24] Jason Hong. "The state of phishing attacks". In: *Communications of the ACM* 55.1 (2012), pp. 74–81.

[25] Md Zahurul Huq and Syed Islam. "Home area network technology assessment for demand response in smart grid environment". In: *2010 20th Australasian Universities Power Engineering Conference*. IEEE. 2010, pp. 1–6.

[26] Yasin Kabalci. "A survey on smart metering and smart grid communication". In: *Renewable and Sustainable Energy Reviews* 57 (2016), pp. 302–318.

[27] Charalampos Kalalas, Linus Thrybom, and Jesus Alonso-Zarate. "Cellular communications for smart grid neighborhood area networks: A survey". In: *IEEE access* 4 (2016), pp. 1469–1493.

[28] Athar Ali Khan, Mubashir Husain Rehmani, and Martin Reisslein. "Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols". In: *IEEE Communications Surveys & Tutorials* 18.1 (2016), pp. 860–898.

[29] Patrick Kinney et al. "Zigbee technology: Wireless control that simply works". In: *Communications design conference*. Vol. 2. 2003, pp. 1–7.

[30] Katharina Krombholz et al. "Advanced social engineering attacks". In: *Journal of Information Security and applications* 22 (2015), pp. 113–122.

[31] Mehmet S Kuran and Tuna Tugcu. "A survey on emerging broadband wireless access technologies". In: *Computer Networks* 51.11 (2007), pp. 3013–3046.

[32] Trong Nghia Le et al. "Advanced metering infrastructure based on smart meters in smart grid". In: *Smart Metering Technology and Services-Inspirations for Energy Utilities*. IntechOpen, 2016.

[33] Suvi Leppänen, Shohel Ahmed, and Robin Granqvist. "Cyber Security Incident Report—Norsk Hydro". In: (2019).

[34] Kratikal Tech Pvt Ltd. *Humans are the weakest link in the information security chain*. 2018. URL: https://medium.com/@kratikal/humans-are-the-weakest-links-in-cyber-security-of-any-organisation-ac04c6e6e71.

[35] Anzar Mahmood, Nadeem Javaid, and Sohail Razzaq. "A review of wireless communications for smart grid". In: *Renewable and sustainable energy reviews* 41 (2015), pp. 248–260.

[36] Rahat Masood, Zahid Anwar, et al. "SWAM: Stuxnet worm analysis in metasploit". In: *2011 Frontiers of Information Technology*. IEEE. 2011, pp. 142–147.

[37] Jeff McCullough. "AMI security considerations". In: *Elster, ref. WP42-1007B* (2010).

[38] V Dhanesh Menon et al. "Cyber Security for Smart Meters". In: *2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*. IEEE. 2019, pp. 1–5.

[39] Guowang Miao et al. *Fundamentals of mobile data networks*. Cambridge University Press, 2016.

[40] Yilin Mo et al. "Cyber–physical security of a smart grid infrastructure". In: *Proceedings of the IEEE* 100.1 (2011), pp. 195–209.

[41] Ramyar Rashed Mohassel et al. "A survey on advanced metering infrastructure". In: *International Journal of Electrical Power & Energy Systems* 63 (2014), pp. 473–484.

[42] Francois Mouton, Louise Leenen, and Hein S Venter. "Social engineering attack examples, templates and scenarios". In: *Computers & Security* 59 (2016), pp. 186–209.

[43] Paul Mueller and Babak Yadegari. "The stuxnet worm". In: *Département des sciences de linformatique, Université de lArizona. Recuperado de:* (2012). URL: https://www2.cs.arizona.edu/collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf.

[44] Nazmus S Nafi et al. "A survey of smart grid architectures, applications, benefits and standardization". In: *Journal of Network and Computer Applications* 76 (2016), pp. 23–36.

[45] Palak P Parikh, Mitalkumar G Kanabar, and Tarlochan S Sidhu. "Opportunities and challenges of wireless communication technologies for smart grid applications". In: *IEEE PES General Meeting*. IEEE. 2010, pp. 1–7.

[46] Olivier Pauzet. "Cellular Communications and the Future of Smart Metering". In: *Sierra Wireless, Inc* (2010).

[47] Scott Poretsky and Brenda Connor. 2021. URL: https://www.ericsson.com/en/blog/2021/6/how-to-use-a-systems-based-approach-to-secure-cellular-iot.

[48] R Santodomingo et al. "SGAM-based methodology to analyse Smart Grid solutions in DISCERN European research project". In: *2014 IEEE International Energy Conference (ENERGYCON)*. IEEE. 2014, 751
bibrangedash
bibrangedash 758.

[49] Mitnick Security. URL: https:\/\/www.mitnicksecurity.com\/blog\/6-types-of-social-engineering-attacks.

[50] Jaydip Sen, Winston Seah, and Yen Kheng Tan. "Routing security issues in wireless sensor networks: attacks and defenses". In: *Sustainable Wireless Sensor Networks* (2010), pp. 279–309.

[51] Jung Taek Seo. "Towards the advanced security architecture for Microgrid systems and applications". In: *The Journal of Supercomputing* 72.9 (2016), pp. 3535–3548.

[52] Manish Shrestha et al. "A Methodology for Security Classification applied to Smart Grid Infrastructures". In: *International Journal of Critical Infrastructure Protection* 28 (2020), p. 100342.

[53] Khaled Shuaib et al. "Resiliency of smart power meters to common security attacks". In: *Procedia Computer Science* 52 (2015), pp. 145–152.

[54] Florian Skopik and Zhendong Ma. "Attack vectors to metering data in smart grids under security constraints". In: *2012 IEEE 36th Annual Computer Software and Applications Conference Workshops*. IEEE. 2012, pp. 134–139.

[55] Florian Skopik et al. "A survey on threats and vulnerabilities in smart metering infrastructures". In: *International Journal of Smart Grid and Clean Energy* 1.1 (2012), pp. 22–28.

[56] Lance Spitzner. *This is Why The Human is the Weakest Link*. URL: https://www.sans.org/security-awareness-training/blog/why-human-weakest-link.

[57] CSU Suganya and C Subhalakshmipriya. "Smart Grid in Electrical and Electronical Communication Technology". In: *International Journal of Engineering Research and General Science* 3 (2015), p. 2015.

[58] Amr Thabet. "Stuxnet malware analysis paper". In: *Code Project* (2011).

[59] Tim Thornburgh. "Social engineering: the" dark art"". In: *Proceedings of the 1st annual conference on Information security curriculum development*. 2004, pp. 133–135.

[60] Ahmad Usman and Sajjad Haider Shami. "Evolution of communication technologies for smart grid applications". In: *Renewable and Sustainable Energy Reviews* 19 (2013), pp. 191–199.

[61] Stilianos Vidalis and Andrew Jones. "Analyzing Threat Agents and Their Attributes." In: *ECIW*. 2005, pp. 369–380.

[62] Wenye Wang, Yi Xu, and Mohit Khanna. "A survey on the communication architectures in smart grid". In: *Computer networks* 55.15 (2011), pp. 3604–3629.

[63] Abdulrahman Yarali and Saifur Rahman. "Smart Grid Networks: Promises and Challenges." In: *JCM* 7.6 (2012), pp. 409–417.