Abstract - A security by design approach for smart metering, using secure design patterns, is introduced in this paper. There are concerns that the security vulnerabilities in smart metering systems can be exploited on a large scale. On an individual level, smart meters can be made to provide false metering data to the service providers. On the collective level, the smart grids can be attacked to bring down the national grid or parts of it, which is a concern of national security. A list of possible security attacks on the smart metering systems is identified and summarized in this paper. It is well known that secure design patterns reduce the design flaws in a system. State of the art smart metering systems do not follow the standardized software development processes. A security pattern based engineering approach for developing secure software for smart metering systems is introduced in the paper. The secure design patterns are stored in a repository of patterns using pattern modeling tools. The engineering process and corresponding modeling tools were developed during the EU project, entitled “Trusted Computing Engineering for Resource Constraint Embedded Systems Applications”.

Keywords - Smart Metering; Security Threats; Security Patterns; Security by Design; Smart Metering Gateways

I. INTRODUCTION

Deployment of smart metering is expected to experience a heavy expansion in the near future. The European parliament has mandated the rollout of smart electricity meters in all the member states by 2022, with 80% rollout due by 2020 [1]. Other developed countries such as USA, Canada, UK and Australia are also investing heavily in smart metering projects and smart meter rollout has already begun in these countries. However, like every automation, this comes with the potential threat of increased technical fraud. Such frauds have already been listed and discussed in other works, e.g., [2]. There are strong conditions and restrictions on the (secure) software / firmware download of metrological software [3]. Many national laws related to online metering exist, covering data protection, privacy, security, regulation of energy and telecommunication, etc. There are also rules and guidelines concerning the metrological aspects of the smart metering systems. However, there are no guidelines or rules for standardized software development of the smart metering systems, let aside the secure software development. This results is the analysis, design and / or implementation issues, which are not given careful thoughts, to be reflected later in the form of security loopholes which are exploited by attackers.

A summary of potential security attacks on smart metering systems are listed in this paper. The recent gateway based approach for smart metering systems is discussed. It has been demonstrated in the software engineering community that secure design patterns can be used to solve the recurring problems of security in a particular domain. A security by design approach, using secure design patterns, to solve the security issues at the early stage in the software development lifecycle of smart metering systems is proposed here. The approach was explored and successfully applied in the project entitled “Trusted Computing Engineering for Resource Constraint Embedded Systems Applications” (TERESA), funded by the European commission, which was successfully completed in 2013.

This paper is organized as follows. Section II explains the smart metering systems. Section III discusses the privacy concerns resulting from smart metering systems. In Section IV, the security concerns, such as the attacker models and the potential security attacks on smart metering systems, are discussed and addressed. A gateway based approach for smart metering systems is discussed in Section V. Section VI discusses the security by design approach in the development process of smart metering systems. An example of a secure design pattern along with the static and dynamic structures is given in Section VII. Finally, the paper is concluded in Section VIII.

II. SMART METERING SYSTEMS

A. Smart Meter

A smart meter is a device installed at the customer’s premises (house or a facility) for measuring the consumption of various commodities such as gas, water and electricity. A smart meter is typically equipped with digital displays and (two way) communication units. It is normally capable of measuring the amount of energy exported as well as imported by the customer, who is not only a consumer anymore but can also produce and sell energy.

B. Smart Metering

Smart metering refers to the smart meters, communication networks and the infrastructure between smart meters and remote entities, such as the energy consumers, meter operators, energy suppliers or the utilities and the meter data management systems. Smart metering data can be used to identify anomalies, energy wasting equipment and offer improvements. Smart metering should support,

• Data acquisition over a Home Area Network (HAN) and communication of the commodity consumption status, in
real time, over a Wide Area Network (WAN) to the utility.

• In House Display (IHD) to show the consumption status to the customer.
• Bi-directional communication capability, reducing physical visits and allowing software updates.
• Scalability and interoperability of equipment supplied by different suppliers, potentially from around the world.
• Generation of load profiles and load schedules.
• Ensuring the security and privacy of consumer’s data.

C. Load Profiles
A load profile is a plot of the variation in energy demand versus time. It helps the power generation companies to predict, in advance, the energy demand over a specific duration of time. Load profiles are extremely important to ensure the availability and reliability of power transmissions to meet the energy demands.

The load profiles were traditionally maintained manually by manually measuring the energy consumption on a monthly basis. The energy suppliers’ obligations are however settled on an hourly or sub-hourly basis, whereas the demand may vary on hourly basis and the load profiles must be built with high probability of demand predictability. Smart meters help in building load profiles to the needed fine grained intervals.

D. Billing and Accounting
Smart metering helps in improved and fine grained billing. With the availability of fine grained consumption information, billing is improved and done on the actual commodity consumption in real time or almost real time. The customer can also see his consumption and can adjust it according to his monthly budget.

III. PRIVACY IN SMART METERING

A. Security vs. Privacy
Security and privacy are not the same. Privacy of information is extremely important in the context of smart metering. Since the data is exchanged over public networks, it is susceptible to being seen or changed in transit by unintended people which could have disastrous consequences for data owners. An example of the fine grained data collection using a smart meter is shown in Fig. 1.

Information security on the other hand addresses issues like confidentiality, integrity, authenticity, non-repudiation and availability. Confidentiality can address the privacy concerns by protecting the customers’ data from unintended recipients.

B. Need for Privacy Protection
A passive adversary with access to the communication between a smart meter or a gateway and the utility can infer useful information from the usage data. By observing the fine grained usage data exchange, the adversary can deduce when the customer wakes up, how many people are at home at a particular instance of time, when do they go to sleep, when do they have their breakfast, when do they watch TV and whether or not they are at home.

It has been shown [4] that even the type of TV programs watched by consumers can be monitored and inferred from the electricity consumption data. In [5] an approach was proposed to identify the actual multimedia content being watched by using the smart meter power usage profiles. The data collected can potentially be used for many purposes, such as, burglary, marketing / advertisement, piracy control, neighborhood check, consumer behavior, monitoring habits of neighbor, intrusion into privacy, etc. There is a need for enhanced privacy protection, which can be handled through confidentiality mechanisms for secure data exchange.

IV. SECURITY IN SMART METERING
In this section we look at the security aspects in smart metering systems and we address those aspects in later section by modeling the secure design patterns. Smart Grid will become an attractive target for various attackers, cyber criminals, terrorists and even hostile nations for a number of reasons. The most common cyber-attacks are breaches of personal data within the network, payment frauds, and denial of service (DoS) attacks on the energy delivery.

A. Attacker Models
Of the most interested attackers in smart metering systems, the following are worth mentioning,

- Eavesdroppers – Listening passively to other people’s communications
- Marketing agencies – Finding out the interests of people
- Customers – Payment frauds
- Novice attackers – Out of curiosity
- Active attackers – This is the most dangerous category of attackers as they could bring down the whole smart metering systems

Figure 1. Example of energy consumption over a period of 24 hours
B. Security Attacks

1) Eavesdropping
Such attacks affect the privacy of a customer by obtaining illegal access to his data or communication over the network. Eavesdropping can be performed over a wireless communication channel or a power line. The detection of such attacks is very difficult. Eavesdropping is most commonly performed through the WAN, e.g., by a curious neighbor or a burglar.

2) Denial of Service (DoS) Attacks
DoS attacks will render the smart metering system unusable for the legitimate users. DoS attacks can either bring down the complete smart grid or part(s) of it. DoS attacks are normally performed in the WAN in many ways, such as by an adversary sending out many more commands than expected to the smart metering gateways or on the other end to the utility servers. The system will saturate and will no more respond to the legitimate requests. It will essentially shut down the grid, completely or partly for essential services to the legitimate users.

3) Packet Injection Attacks
These attacks are launched by injecting false packets, e.g., false commands for a smart meter, into the network. Packet injection attacks are mainly performed through the WAN. They might be used to cut down power to parts of the smart metering system or to compromise the billing process by generating false bills resulting in financial losses.

4) Malware Injection Attacks
Such attacks are normally launched by injecting malware into the network/WAN, effecting the communication between devices and compromising the billing and reporting processes. The demand/consumption status of the grid might be disrupted to destabilize the load on the grid.

5) Remote Connect/Disconnect
The remote connect/disconnect facility of the smart grid can be exploited by furious attackers, bringing the grid or its components to halt. If launched on a massive scale, this attack can leave a lots of users disconnected from the commodities such as electricity, gas or water supplies. These attacks are normally launched via the WAN by injecting false command packets into the network.

6) Firmware Manipulation
Firmware manipulation involves changing either the metrological or the non-metrological part of a smart meter or a gateway. If the metrological part is manipulated, the attacker can disrupt the billing and accounting process of the target, e.g., by reporting false consumption status. The firmware manipulation can either be performed by physically accessing a smart meter (gateway) or accessing it through the WAN. Such attacks can affect a single user but they can also be launched on a massive scale, e.g., by remotely manipulating the firmware of a large number of gateways.

7) Man-in-the-Middle Attacks
In a man-in-the-middle attack, an attacker “inserts” himself in the middle of communicating parties, capturing their messages and by relaying them to the other end, making each of them believe that they are talking directly to each other. Thus the attacker can either passively eavesdrop or modify the information being exchanged between the communicating partners. A man-in-the-middle attack can be launched inside the Local Metrological Network (LMN) or the WAN. If launched inside the LMN, this attack can be used to compromise the communication between a meter and a gateway and to provide false feedback to the gateway from a meter, e.g., to provide false consumption status.

If the man-in-the-middle attack is launched through the WAN, the security and privacy of legitimate communicating partners can be compromised on a large scale, e.g., the communication between a gateway and remote readout center (RRC), thereby revealing a lots of information about the energy consumption in a premises and thereby the information about the people in the premises. The commands from the authorized remote entities to gateways can be forged and spoofed by attackers as well. Fig. 2 depicts the possible security attacks and their targeted locations.

V. Gateway Based Approach
Smart metering gateway is a part of the recent approach to smart metering proposed by European countries, including Germany and the UK. A gateway is an enabling technology and the most important component for future communications between the smart devices in the customer premises (HAN) and the utility via WAN. The HAN has end consumer devices, such as a display console for the consumer, smart electric heaters, washing machines, Fully Electric Vehicles (FEV), etc.

A gateway is responsible for the smart meters and other smart devices installed in a house/premises. The gateway periodically communicates the consumption information to the utility servers via WAN. The gateway also gets instructions from the load distribution controller in the smart grid. A smart metering gateway interacts as a part of the smart grid. It should therefore have the capability to support many different communication protocols and standards such as PLC, RS-485, Zigbee, MBUS, Wireless MBUS, GSM, GPRS, PSTN etc.

![Figure 2. Security attacks](image-url)
In Germany, the German Federal Office for Information Security (or Bundesamt für Sicherheit in der Informationstechnik (BSI)), proposed the smart metering architecture shown in Fig. 3 [6]. It comprises of a gateway for communication from LMN / HAN to the WAN and is responsible for security. The gateway includes one or more smart meters and connects the WAN, HAN and the LMN. The gateway also consists of a communication module for communicating over the WAN by transmitting the consumption information and accepting commands from the remote end. Additionally, the gateway has a hardware security module to ensure the security of data and communication over the network.

The architecture for the interconnection of smart metering devices, proposed by the Department of Energy and Climate Change in the UK [7], is shown in Fig. 4. The “Communications Hub” in this architecture has essentially the similar responsibility as the smart metering gateway proposed by the BSI PP. There is a minute difference that the HAN includes the LMN as well as the end user devices. Like the BSI PP approach, the communications hub is connected to a WAN as well as a HAN.

**VI. SECURITY BY DESIGN APPROACH**

**A. Need for Security by Design**

Due to the large scale of the smart metering systems and the smart grid infrastructure, there is a need for security by design approach while developing the smart metering systems. Though the support for remote software / firmware update to fix the security and other bugs is envisaged for smart meters and smart metering gateways, due to the criticality of the systems and its ultimate impact on a nation’s security, it might be too late to react after an attack has been launched. Security by design is a group of concepts and means to induce security in a system by design rather than as add-ons when security loop holes and exploits are discovered. This means that the software and hardware systems for smart meters should be developed based on security analysis, security design, secure implementations and security testing in parallel to the analysis, design, implementation and testing of other system components.

In [8], a systematic method for modeling the functionalities of smart meters and a way to derive attacks that can be mounted on them was shown. The authors showed how attacks can be identified using the abstract model (behavior) of the software and then mapped to concrete model (actual implementation). An open source meter was used and two real attack scenarios were implemented, named as the communications interface attack and the physical memory attack. This approach shows that if the software of the smart metering systems is not designed with security considerations in design, the attacks can always be done very systematically.

In the TERESA project [9], it was shown how security can be embedded into all (or most of) the phases of the software development lifecycle, right from the requirements and analysis phase up until the implementation and testing phases, using secure design patterns. The results were applied and tested for smart metering gateways developed in accordance with the Germany’s BSI PP approach [6]. A prototype was developed to show the applicability of the idea. If security is made a part of design, then many security issues can be solved through previous experiences gained from known security loop holes.

**B. Secure Design Patterns**

A pattern is a general reusable solution to a commonly occurring problem in design [10]. Design patterns for software development were popularized in [11] where a large number of design level patterns were published aimed at object oriented programming. Secure design patterns, for aiding in secure software development were introduced in [12]. Using a pattern based design and development approach also helps in retaining and reusing the expert knowledge in a particular domain, reducing the risk of vulnerabilities being introduced while re-designing or re-implementing a known component of a system.

It was demonstrated that many flaws arising from loopholes in the analysis, design and especially in the software development phase can be avoided if pattern based security engineering approach is used. By carefully considering the already discussed security attacks in the analysis and design phase, the well-known attacks can be prevented. A careful thought in development and thoroughly tested patterns will also reduce the future attacks. Additionally, the commercial benefit is that the time to market a product is reduced significantly as well.
C. Engineering Process

The engineering process adopted to develop the smart meter gateway in TERESA is based on the V-Model. It involves, requirements analysis, system design, architectural design and implementation, followed by unit, integration and system testing. The last phase is evaluation and certification based on the Common Criteria. Secure design patterns are used in each phase of the V-Model, making the task of evaluation and certification easier and faster.

D. Repository of Security Patterns for Smart Metering Gateway

In TERESA project, a diverse repository of security patterns was developed and tested for the smart metering gateway using the BSI PP approach [6]. The gateway is a central and important component as it controls the traffic to and from the WAN and therefore most of the secure design patterns were focused on the Gateway. The following security patterns were developed in TERESA,

- **Secure Remote Readout** – To securely perform the task of remote readout
- **Key Manager** – To perform the task of key management securely
- **Wakeup Service** – To react to the connection establishment from the remote readout center for pull readout operation
- **Transport Layer Security** – A pattern for the Transport Layer Security (TLS) operations
- **Secure Logger** – To securely maintain log on the gateway

These patterns are modeled at different levels, such as analysis, design and implementation level and stored in a repository of patterns using the modeling tools developed during the project based on the Eclipse modeling framework. The modeling tools also provide the ability to perform basic testing and formal validation on the developed patterns. The repository based approach is shown in Fig. 5.

VII. Secure Remote Readout (SRR) – An Example Security Pattern

A. SRR Pattern

Out of the security patterns mentioned in Section V.D, one pattern, SRR, is described here due to space limitations. The SRR pattern is modeled at the requirements, analysis, design and implementation phases of software development lifecycle (V-Model). This gives an insight into the idea and how the pattern based engineering approach can be effectively applied.

B. Pattern Description

Pattern description is based on the standard representation developed in [11].

**Name:** Secure Remote Readout

**Aliases:** Remote Readout, Read Measurement

**Context:** A remote entity (such as a utility) needs to know the status of commodity consumption on regular basis.

**Problem:** Measurements from the gateway to the remote entity need to be transmitted securely.

**Solution:** To counter the privacy and security issues over insecure WAN, the gateway uses cryptographic mechanisms with the help of a dedicated hardware (Security Module). The security module provides cryptographic functionalities, such as, en-/decryption, digital signatures, key generation and secure key storage. The measurements are digitally signed using the private key of the gateway and encrypted using the public key of the remote entity. All the data is exchanged using a Transport Layer Security (TLS) connection between the gateway and the remote entity.

**Structure:** The static structure of the components involved in SRR is discussed next in the class diagram.

C. Class Diagram

Class diagram of the SRR pattern is shown in Fig. 6, which depicts the static structure of the pattern. The metering measurements of different commodities go from a meter via the gateway to the remote readout center.
The measurements are then digitally signed and encrypted for integrity and confidentiality protection, ensuring the security and privacy of the data in transit. For this purpose a security module (a physical device in BSI PP [6]), is used to perform the cryptographic functions and secure data storage. Communication between gateway and RRC is performed using TLS. TLS itself, is developed as another pattern, which is used by the SRR pattern.

D. Interaction

The interaction between different patterns is captured through the sequence diagram, as shown in Fig. 7. In case of the described system, a Meter pattern gives its data to a Gateway. The gateway is responsible for communication over the WAN, with the Remote Readout Center. The data is digitally signed and encrypted by gateway using a security module. Since the BSI model was used, therefore, a hardware based security module was used instead of a software library. The Gateway establishes a TLS connection to the RRC and sends the encrypted and digitally signed measurement to the Remote Readout Center. Note that the data in this approach is dually encrypted, using a Security Module as well as TLS, because TLS alone is not considered secure anymore after recent attacks on TLS. The Key Ring provides access to the keys shared between Gateway and other communication partners, e.g., Meter and RRCs.

VIII. CONCLUSION

A list of potential security threats and attacks on smart metering systems is evaluated in the paper. Security solutions for smart metering systems are presented, including the gateway based approach as proposed by the BSI PP. The need for a security by design approach is emphasized. A security pattern based engineering approach for smart metering gateways is proposed. Secure design patterns are modeled at different levels of the V-Model for software development and the patterns are stored in a pattern repository using the modeling tools. The repository is used by pattern developers, thereby benefiting from the experience of security experts and reducing the development time and the time to develop and market the product.

REFERENCES