FAKULTÄT
FÜR !NFORMATIK
Faculty of Informatics

Sichere Architektur für Smart Hubs

BACHELORARBEIT

zur Erlangung des akademischen Grades

Bachelor of Science

im Rahmen des Studiums

Technische Informatik

eingereicht von

Viktor Ullmann
Matrikelnummer 00925881

an der Fakultät für Informatik
der Technischen Universität Wien
Betreuung: Ao.Univ.Prof.Dr. Wolfgang Kastner

Wien, 8. Juni 2018

Viktor Ullmann	Wolfgang Kastner

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Security Architecture for Smart Hubs

BACHELOR'S THESIS

submitted in partial fulfillment of the requirements for the degree of

Bachelor of Science

in

Computer Engineering

by

Viktor Ullmann
Registration Number 00925881

to the Faculty of Informatics
at the TU Wien
Advisor: Ao.Univ.Prof.Dr. Wolfgang Kastner

Vienna, 8th June, 2018

Viktor Ullmann

Wolfgang Kastner

Erklärung zur Verfassung der Arbeit

Viktor Ullmann
Gersthoferstraße 86, 1180 Wien

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 8. Juni 2018

Viktor Ullmann

Danksagung

Ich danke Nora, meinen Eltern und meinem Betreuer, Wolfgang Kastner.

Kurzfassung

Mit zunehmender Zahl an smarten Geräten in den Haushalten steigt der Bedarf, auf diese Geräte in einer einheitlichen Schnittstelle zuzugreifen und sie zu steuern. Smart Hubs ermöglichen dies. Diese Arbeit zielt darauf ab, Design-Vorschläge für Smart Hub Entwickler bereitzustellen. Um die Benutzer vor Attacken und Datenmissbrauch durch Angreifer zu schützen, müssen Informationssicherheit (Security) und Datenschutz (Privacy) von Beginn an in Design und Entwicklung bedacht werden. Dafür wird eine Analyse der Normen und Richtlinien der EU und EU-Mitgliedsstaaten in Bezug auf Security und Privacy präsentiert. Aus diesen Regulatorien werden Anforderungen für die Entwicklung eines Smart Hubs abgeleitet. Abschließend werden bewährte Methoden und Entwicklungsdetails zur Implementation eines Smart Hubs präsentiert.

Abstract

With the increasing number of smart devices deployed in our homes, the need to access and control them in a single device grows. Smart hubs fulfill this need. This work aims to provide design guidelines for smart hub designers. To protect users from malicious attacks and data abuse, security and privacy aspects need to be included in the design and implementation from the very beginning. To this end, an analysis of regulations, mainly EU-wide and EU-country specific, regarding security and privacy is provided. From there, requirements for the development of a smart hub are derived. Finally, best practises and implementation details are presented to the reader.

Contents

CHAPTER 1

Introduction

The current smart home environment is very heterogeneous, with competing standards and protocols or devices using proprietary communications rarely adhering to any standards [1]. Furthermore, smart meters are starting to be rolled out across the EU member states. These are power meters that provide digital interfaces for remote meter data collection and other related services to the grid operator as well as the building owner and authorized 3rd parties. To use all devices and different smart meters in a single interface and to automate the home using diverse devices, an abstraction layer was introduced. A smart hub realizes this abstraction, by integrating all smart devices and providing the user with the ability to control them through a single interface. A smart hub provides great utility to the user, but also introduces a security risk. If an attacker manages to take over a smart hub, they have the ability to cause damage to the house, violate the privacy and security of the owners, cause increased cost for the owners or, in the worst case, if a large number of smart hubs can be controlled, cause damage to the power grid.

This document aims to aid developers of smart hubs (and smart devices to some extent) in developing a secure platform for the users. In order to provide a complete overview of all development stages, regulations for smart devices in Europe are analyzed and summarized, important attack surfaces are highlighted and technical implementation guidelines laid out for the developers of a smart hub.

The recommendations in this document are targeted for the European market. Therefore, different legal standards and frameworks of different member countries apply. Some of them are required by law, others are considered as recommendation. As smart hubs will be connected to smart meters and other services provided by the smart grid infrastructure in the future, the stricter smart grid regulations must be taken into consideration. To harmonize the different security frameworks of the member countries, the standards are summarized to provide an overview of applying regulations.

After that, a proposed course of integration of cybersecurity and data privacy solutions is described, as well as possible security testing technologies, procedures, and results.

Finally, the practical implementation is covered with some details on how to implement various features and security measures.

1.1 Smart Home Ecosystem

The current smart home market is highly diverse, with many competing standards for controlling of the smart devices [2]. It is therefore necessary to have a device that abstracts the different underlying communication protocols and provide a unified, transparent user interface for controlling all smart devices in a household.

The following listing gives an overview of some current smart home communication protocols and technologies which are used to interconnect smart devices [1].

- **ZigBee**

  ZigBee is a smart home standard working with smart devices from companies like Miele, Philips and Osram. The focus of this system is home automation, medical engineering and industrial automation hardware. It is based on wireless communication for devices with minimal energy consumption and minimal amount of data. ZigBee collaborates with about 230 different companies. [3]

- **Z-Wave**

  Z-Wave is a smart hub system with a wide range of controllable devices like energy meters, lighting and entertainment systems, door locks, sensors, thermostats and many more. Z-Wave is implemented on a system-chip (SoC) combined with a microcontroller and radio-transceiver. It has collaborations with over 600 companies, for example companies like Siemens and Nokia. [4]

- **KNX**

  KNX is an open network communication standard mainly used for building automation. The choice for physical media is diverse, with radio, powerline and twisted pair as possibilities. Main advantage of this standard is the flexibility from low- to high-level infrastructure and large number of supported devices and applications (e.g. window blinds, switches, alarm systems, access control). [5]

- **WiFi**

  WiFi is a known and proven technology to enable communication between devices. Smart home systems from companies like Amazon, Apple and Google are constructed to work with this communication standard. Generally in smart homes, a combination of WiFi and other radio technologies make a good working structure.

- **EnOcean**

  EnOcean is another wireless communication standard, specialized in monitoring, home and facility engineering. The unique characteristic of EnOcean sensors and switches is that they are mostly functioning without the use of power. EnOcean developed a solution based on "energy harvesting" (e.g. based on piezoelectricity). They work with about 250 companies, for example Siemens, Zumtobel, Texas instruments and ABB. [6]

1.2 Importance of Security in Smart Home Devices

A smart hub with a number of loads connected to it introduces several risks to the building owner. The following section expands on previously mentioned risks, gives an overview on what the risk is and the associated damage potential [7].

1.2.1 Cause Physical Damage

An attacker can cause damage to the owner's property by switching connected loads in ways not intended. For example, an attacker could switch a device on and off in a high frequency, exhausting the typical lifespan. Another attack could be switching devices that should be mutually exclusive, for example running heating and cooling at the same time, bringing both systems to their maximum load. An indirect damage could be caused by simply opening a smart door lock and disabling the alarm system, allowing burglars to enter without any obstacle.

1.2.2 Increased Cost

By switching heavy loads and overriding set points, an attacker can cause increased energy usage leading to higher cost for an owner. Again, an example would be to turn on cooling and heating at the same time, causing them to use maximum power.

1.2.3 Privacy and Security

Smart hubs gather energy usage data to provide convenience or energy management services to the user. When a smart hub is compromised, or the communication can be monitored by an attacker, it is possible to observe private usage data. The most basic data point that can be obtained is whether anyone is in the building, e.g. by the state of lighting or the use of a presence sensor. This could provide burglars with information on when to break into a building without having to be on-site and observe the house. From usage analysis, especially in conjunction with a high sampling resolution smart meter, much more information can be gathered [8]. Another issue, although true for every connected device, is that the attacker can use a vulnerable device as a so-called jump host. This means the device is an entry-point to the private network otherwise protected by a firewall. From there, other services on the network can be attacked (for example, smart phones, data storage).

1.2.4 Power Grid

If an attacker can switch loads simultaneously over many homes connected to the power grid, coordinated load switching can cause severe damage to the whole power grid [9]. This damage potential opens opportunities for organized crime (e.g. extortion) or terrorist attacks. A homogeneous environment with many smart hubs of the same model deployed heightens that risk as an attacker can leverage a single exploit to access a large number of devices.

CHAPTER 2

Security by Design

Adding security after the fact can be challenging, and some shortcuts might need to be taken to retrofit security. Therefore, the "Secure by Design" paradigm should be applied. Generally, this means that security is regarded as basic functionality of the smart hub. The acts of an attacker are anticipated and considered from the beginning of the project, taking the necessary precautions to prevent an attacker from succeeding in their attack.

2.1 Secure Development Lifecycle

A central role in the development of a smart hub is the security, ranging from a secure design over implementation security to operational security. It is thus necessary to follow a Secure Development Lifecycle (SDL) (Figure 2.1).

2.1.1 Security Requirements

In the first step, it is essential to define the security and data privacy requirements to identify the necessary security functions for the smart hub design and in the subsequent hardware and software implementation of this design.

2.1.2 Design and Implementation

In the next step, a “secure by design” solution is developed. Once the design is complete, the implementation of the design can start. Through the technical implementation it is necessary to adhere to established implementation security guidelines and practices to avoid technical vulnerabilities. For instance, a “secure by design” system could include a set of cryptographically secured authentication messages that are exchanged between devices. While this message exchange itself could be “secure by design”, the actual software implementation of the message exchange handling code could include a software vulnerability such as a buffer overflow flaw which would jeopardize the security

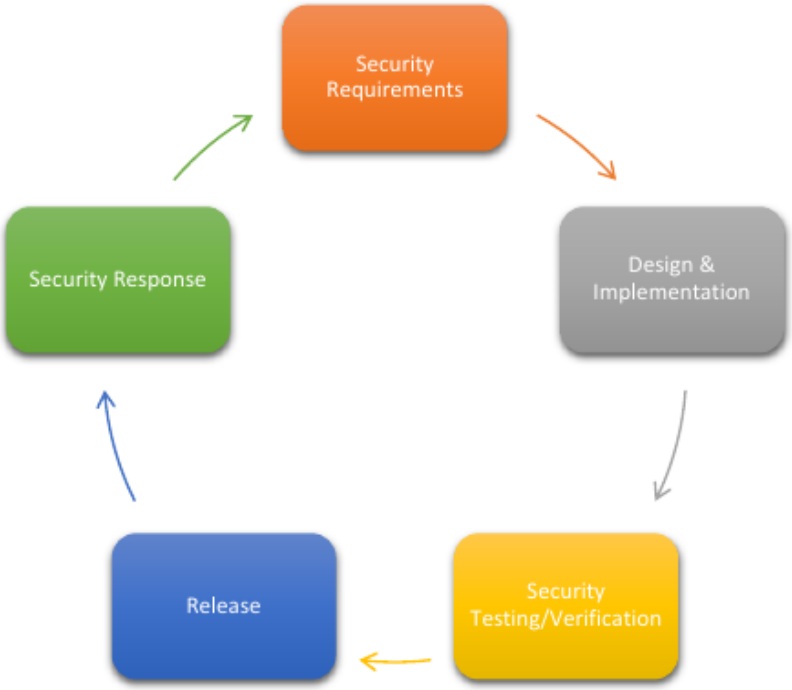

Figure 2.1: Cyclic process view of a Secure Development Lifecycle (SDL)

of the overall system. Proper security training of the developers and building up upon established implementation security guidelines and practices minimizes implementation flaws. Ultimately, these techniques can significantly lower the likelihood of vulnerabilities but at the same time it is impossible to prove the correctness of the system or the absence of vulnerabilities (undecidability/halting problem).

2.1.3 Security Testing/Verification

Once the design has been implemented, it is necessary to perform security tests on the actual implementation. An important goal during these tests is to (1) verify that the implementation actually performs the security functions defined in the design, and (2) test the robustness of the hardware and software implementation with regard to common implementation security flaws. In addition to common software implementation vulnerabilities and attacks, Figure 2.2 provides an overview of physical hardware implementation attacks that are in particular necessary to consider since the smart hub will be located within the customer's premises and thus easily accessible by potential adversaries. While for software implementation security testing established analysis tools can be utilized, the hardware security testing approach needs to be specifically backed by the development of suitable testing and auditing technologies.

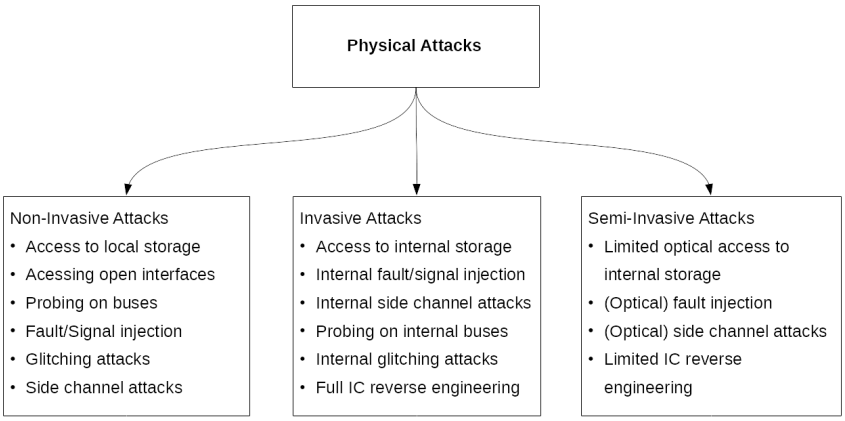

Figure 2.2: Overview of physical implementation attacks [10]

2.1.4 Release

In this step, the solution has been already thoroughly scrutinized and it is released to the customers. This state is idle, a discovered vulnerability leads to the next step in the SDL.

2.1.5 Security Response

Even though the likelihood of vulnerabilities has been significantly lowered through security tests and validation, it is still possible that vulnerabilities are discovered. The security response process allows addressing this case so that subsequent security fixes and patches can be created throughout the cyclic SDL process.

CHAPTER 3

Regulatory Framework for Smart Hub Systems

The general aim of this thesis is to provide guidelines for the development of a smart hub system which is targeted to be used in the European Union. Therefore, it is important to outline the legal standards of every country and combine them to a standardized solution for the smart hub architecture.

To build a smart hub architecture which also complies to the strictest member country regulatory policies, it is recommended to adhere to the strongest and most detailed frameworks for the smart hub solution. This also ensures a high security standard in other countries with less strict regulations.

The regulatory frameworks of EU countries are considered to ensure that all existent legal dispositions are met. Similarly, the functional requirements are addressed to ensure that the security requirements and their subsequent implementation match the aspired solution. This regulation and also regional standards from all member countries of the European Union considered, the smart hub is to be developed according to common criteria as well, see section 3.4.

The European Union currently does not define specific and obligatory security requirements, but instead focuses on security recommendations. In addition to these regulatory frameworks, the following relevant security standards will be used as key inputs:

- ENISA Smart Grid Security Recommendations [11]
- BSI Protection Profiles [12]
- CEN-CENELEC-ETSI Framework [13]
- NISTIR 7628 Guidelines for Smart Cyber Security [14]

- Common Criteria [15]

3.1 ENISA Smart Grid Security Recommendations

The European Union has conducted a study resulting in 10 security recommendations defined in the "ENISA Smart Grid Security Recommendations" [11]. The ENISA is the "European Network and Information Security Agency (ENISA)" with information security expertise for the EU region. Since it is very likely that the member countries will adhere to these security recommendations, they should be considered in the architecture of a smart hub.

In general, the ENISA Smart Grid Security Recommendations are high-level and non-technical security recommendations suggesting, for instance, the collaboration with ENISA, the promotion of the development of security certification schemes or the creation of security test beds and security assessments. Additionally, there are five annexes containing more detailed information and results of the study. Since the recommendations are non-technical in general, based on the high level key findings and general recommendations, the following technical requirements can be derived:

- End-to-end security approach at all levels of communication (see ENISA document section 3.1.3):

  Following from this recommendation, the technical requirements are the cryptographic primitives providing at least confidentiality and integrity as well as the creation of cryptographic keys, the secure negotiation and/or exchange as well as disposal.

- Mandatory risk-driven security assessments (section 3.4.2):

  It implies that technical security auditing methodologies and technologies need to be available enabling device-oriented security assessments.

- Data protection and secure data handling (section 3.7.3):

  Similar to the end-to-end security approach, the technical requirements are the cryptographic primitives providing at least confidentiality and integrity as well as the creation of cryptographic keys, the secure negotiation and exchange as well as disposal.

- Technical challenges (section 3.7.5):

  Following from this recommendation, the interaction with security devices should be based on defined standard interfaces. Segmentation should be taken into account and traffic analyzers should be available (important e.g., for security auditing methodologies and technologies). Moreover, logging, monitoring, trust and authentication capabilities should be existent.

- Assessing product security (section 3.9.6):

  Compared to the technical challenges and risk driven security assessments, the technical requirements need to support security auditing methodologies and technologies to enable product security assessments over a large part of the lifecycle of the smart grid system.

- Technical aspects of cybersecurity incident detection (section 3.10.4):

  Technical requirements for security monitoring sensors with central monitoring, signature-based software in sensors and IDS systems should be present.

The ENISA Annex II "Security Aspects of Smart Grid" document [16] focuses on threats in the smart grid. It provides information regarding security standards and guidelines and should be considered in the architecture of a smart hub system.

The ENISA Annex IV [17] focuses on related technical and non-technical security standards and guidelines.

3.2 BSI Protection Profiles

The BSI protection profiles [12] [18] and their concretizations, as listed below, are guidelines developed in Germany that contain detailed security requirements which are also legally binding in Germany.

- Protection Profile for the Gateway of a Smart Metering System (Smart-Meter-Gateway PP), BSI-CC-PP-0073-2014
- Protection Profile for the Security Module of a Smart-Meter-Gateway (Security Module PP), BSI-CC-PP-0077-V2-2015
- Technische Richtlinie TR-03109 [19]
  - BSI TR-03109-1 – Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems Version 1.0
  - BSI TR-03109-2 – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls", Version 1.1
  - BSI TR-03109-3 – Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen - Version: 1.1
  - BSI TR-03109-4 – Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways - Version: 1.2.1
  - Technische Richtlinie TR-03109-5, Kommunikationsadapter, Status: Document TR-03109-5 in planning stage
  - TR-03109-6 - Smart Meter Gateway Administration - Version: 1.0

- BSI TR-03116-3 Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3, Stand: 2018
- Zertifizierungsrichtlinie Certificate Policy für die Smart-Meter-PKI; Version 1.1.1

The Protection Profile (BSI-CC-PP-0073) [12] defines the security objectives and corresponding requirements for the gateway of a smart metering system. The gateway is the central component for communication between the user and the outside world. The main focus is the protection of confidentiality, authenticity, integrity of data and information flow control to protect the privacy of consumers, to ensure a reliable billing process and to protect the smart metering system. The availability of the gateway is not addressed by this Protection Profile (short PP).

Therefore, various requirements which are defined in this PP should be used in order to build a secure smart grid architecture.

Security auditing should be a mandatory requirement. The log data (system, audit, consumer, calibration) must be protected by alarms from loss and further be auditable. Also audit events shall be associated to the user which caused the event.

In terms of communication the transmitted meter data shall be protected by a hash/signature to verify the origin and validity of the data.

There has to be a certain standard in cryptographic support which means the cryptographic keys (TLS, CMS, communication) and signatures shall only be generated accordingly to BSI-TR-03109-3 and utilize a security module and also be destroyed when no longer in use.

Another important term is the protection of user data. The BSI Protection Profile states that all operations with an external entity over WAN, HAN or LMN with an object of the gateway (any information that is received, transmitted, relayed or stored) shall be covered by an access control mechanism. Furthermore, the gateway shall enforce a firewall on connections with external entities on an interface and authentication level based configurable rule set. Received meter information shall be validated according to information security attributes, processing profile, time synchronization constraints (3% deviation of measuring period), integrity, authenticity and confidentiality. Replay detection and reliable time stamps shall be implemented in the system. In order to protect user data, previous information content of a resource shall be made unavailable if no longer in use by any objects. Likewise, stored data shall be monitored for integrity and covered by action if a data integrity error is detected.

Identification and authentication is a requirement in designing smart systems to make sure only licensed parties have acces to their specific functions or tasks. Therefore, a connecting user shall have the following user attributes: User identity, status of identity (authenticated or not), connecting network (WAN, HAN or LMN), role membership and other security attributes if available. In parallel, a user authentication (via certificates, passwords, etc.) is required before any security relevant action can be taken. Unsuccessful

authentications, between 3-10 failed attempts, shall be detected and dealt with. Re-authentication is dependent on connection/inactivity time, the connected channel or data volume transmitted.

Concerning security management functions like reading version number, current time, firmware updates, deletion or modifications of events in logs, etc. shall only be available for an authenticated user and defined role. Security relevant modifications shall only be performed by gateway administrators.

Regarding privacy, it shall be enforced that no personally identifiable information can be obtained by an analysis of the communication data characteristics. Further, pseudonymity shall be provided for data which is not billing relevant or a secure operation.

To ensure the protection of security functions, a self testing suite shall be provided, running on initial start-up, at request and periodically during normal operation. Additionally, a passive detection of a physical attack shall be provided (seal and appropriate physical design) to verify the physical integrity.

It is also required to provide a secure and trusted channel (confidentiality, integrity, and authenticity) for WAN and meter communication.

The second document, called Protection Profile for the Security Module of a Smart Meter Gateway (BSI-CC-PP-0077, [18]), defines the security objectives and corresponding security requirements for a security module that is utilized by the gateway for cryptographic support. Typically, a *Security Module* is realized in form of a smart card (but is not limited to that).

According to the PP BSI-CC-PP-0077, the parameters for cryptographic support (key generation, destruction and crypto operations) can be realized with the following technical and cryptographic measures:

- ECC-Key pairs generation
- Diffie-Hellman key agreement (TLS)
- ElGamal key agreement (content encryption)
- PACE (Password Authenticated Connection Establishment)
- Signature generation and verification
- Import of public keys
- Secure Messaging (AES CBC, AES-CMAC)
- Random number generation

In terms of user data protection and access control, the PP states that any operations between a subject and an object shall be covered by an access control policy. User data stored in containers shall be monitored for integrity errors on all objects and not be used in case an integrity error occurs. The connected entity shall be warned that such an error occurred. Furthermore, previous information content of a resource shall be made unavailable if no longer in use by any objects and the export of data without associated user security attributes shall be possible, but enforced upon export. The import of user data without security attributes shall be possible and may be ignored if data is not a controlled object by the secure module. And final, the transmission and reception of user data shall be protected from unauthorized disclosure while transmitted and the access control policy shall be enforced. The module shall also be able to determine if a modification, deletion, insertion or replay error occurs.

Moreover, identification and authentication should be secured with the following regulations. The user security attribute has to contain which mutual authentication method was performed, it also should be able to determine if the PACE-PIN is of a required minimum length. Some data fields and functions may be accessed without user authentication. It shall be required that any mediated functionality on behalf of a user is authenticated by an identified user. Authentication of gateway administrators shall be performed by certificates. Additionally, the authentication data using PACE and key-based protocols may not be reused and the module shall provide multiple authentication methods (PACE and key-based).

A set of security management functions and roles should be defined for the smart grid and after deploying the module no test features are allowed to disclose or manipulate user or security related data which may enable other attacks.

The protection of the security module should imply protection from side channel attacks (emissions and circuit surface) to prevent leakage of cryptographic material or other states which may lead to different attacks. The secure state shall be preserved even in the case of power loss, malfunctions, physical manipulation or probing, etc. It shall resist physical manipulation and physical probing. Furthermore, a self testing suite shall be provided, running on initial start-up, at request and periodically during normal operation.

Regarding trusted path/channels it should be made sure that the the security module provides a secure communication channel, assures identification of its end points and provides protection of the channel data from modification or disclosure. Other IT products may initiate a trusted channel. A secure channel shall be enforced on data exchange with the gateway except reading data fields with technical information.

3.3 The CEN-CENELEC-ETSI Framework

The CEN-CENELEC-ETSI Smart Meters Coordination Group has issued a three-part privacy and security approach describing privacy and security requirements for smart metering systems. The first part defines a set of security use cases, for example providing

meters with necessary key material for encrypted communication. The document suggests specific cryptographic algorithms and cipher suites which can be used for the asymmetric key exchange, digital signatures and symmetric encryption like the following listed: [13]

- ECDSA (Elliptic Curve Crypto based Digital Signature) scheme for providing strong authentication of metering data and commands/controls (FIPS PUB 186-3)
- ECDH (Elliptic Curve Crypto based Diffie Hellman) key agreement for establishing a common shared symmetric key between trusted partners (NIST SP 800-56A)
- NIST standard named Elliptic curves P-256 and P-384, providing a common set of domain parameters over a prime field, for the purpose of interoperability of the crypto-operations
- Suite B Implementers' Guide to FIPS 186-3 (ECDSA)
- Suite B Implementers' Guide to NIST SP 800-56A (ECDH)
- AES 128 GCM (Galois/Counter Mode) cipher-suite and cipher suites defined in DLMS COSEM protocol standard (IEC62056 series) (i.e., approved ciphers/algorithms defined in NSA suite B, NIST, FIPS)

In terms of data and message protection, the first part of the CEN-CENELEC-ETSI framework describes the importance of a separation between message protection and data protection. Also end-to-end security and a differentiation between security levels is a demanded standard.

The second part focuses on non-technical requirements and was thus not relevant for the definition of technical security requirements.

Part three of the CEN-CENELEC-ETSI framework mentions both organizational and technical security measures and focuses on security threats and certifications.

As for this document, the following exemplary technical measures have been identified:

- End-to-end encryption
- Certificates
- Use of an automated system to signal connection disruptions
- Use of two factor authentication mechanisms etc.
- Tamper proof smart meters

3.4 Common Criteria

Common Criteria is a three-part standard for audit, evaluation and verification of security features of IT products. It is an international and worldwide known standard (ISO 15408) for security testing and validation.

Part one of the common criteria contains a general model for security evaluation. The second part describes the functional requirements of IT products and the third part provides assurance requirements.

This document defines several classes of functionality to compare them with seven classes of reliability in order to evaluate and certify the IT product. The functional components of this evaluation are broken up into the following classes:

- **Security audit** (class FAU) This class defines internal security auditing like automatic response, data generation, audit analysis, event selection and event storage.
- **Communication** (class FCO) The class communication describes the specifications for a secure exchange of data, particularly the non-repudiation of origin and non-repudiation of receipt.
- **Cryptographic Support** (class FCS) This class includes necessary cryptographic support functionality, such as cryptographic key management and operations. This functionality is especially critically as many of the other security functions build up upon the correctness of these functions.
- **User Data Protection** (class FDP) The user data protection class defines security functions for handling user data in the target of evaluation (TOE). It contains information about user data import, export, storage and security attributes for user data.
- **Identification and Authentication** (class FIA) This class contains security functions necessary to verify the user identity and furthermore to ensure that users are associated with their specific security attributes. It defines functions such as authentification failures, user attribute definition, specification of secrets, user authentication and identification and user-subject binding.
- **Security Management** (class FMT) The security management class defines the functions such as security policies, access control and capability lists, security permissions and roles.
- **Privacy** (class FPR) The class privacy determines all functions related to privacy issues, for example anonymity, pseudonymity, unlinkability and unobservability.
- **Protection of the TOE Security Functionality (TSF)** (class FPT) The Protection of the TOE Security Functionality class is concerning the integrity and

management of the security function data itself. This implicates for example the availability, integrity and confidentiality of exported TSF data, physical protection of the TSF, replay detection, time stamps and self testing.

- **Resource Utilization** (class FRU) This class defines the necessity of defined resources like processing capability and storage capacity. It contains definite terms for fault tolerance, priority of service and resource allocation.
- **TOE Access** (class FTA) The TOE access class provides information for the requirements to control a user session. There has to be a limitations on scope of selectable attributes and the number of concurrent sessions. Furthermore, regulations of TOE access banners, access history and session establishment are described.
- **Trusted Path / Channels** (class FTP) This class defines the terms to assure a trusted communication between the user and the TSF.

The common criteria standard provides a precise basis for security testing requirements in order to build a secure architecture of a smart hub system. Requirements which can be extracted from Common Criteria are included in chapter 4.

3.5 NISTIR

The National Institute of Standards and Technology Interagency Report (NISTIR) composed a guideline for Smart Grid Cyber Security, short NISTIR 7628. Although this standard is a non-European document and therefore not binding in Europe it is mentioned because it presents valuable information in terms of requirements to build the architecture of a smart hub.

Part one of the standard identifies the possible security risks and based on those, develops suitable security requirements for the architecture of a smart hub system. The second part addresses privacy issues and potential risks. The third part consists of supporting analyses and references to the first two parts.

3.6 Regulatory Framework in Austria

Completing the regulatory formwork of the European union, a short overview of the security standards in Austria is followed. The requirements in terms of privacy and security are are loosely defined in the “Gesamte Rechtsvorschrift für Intelligente Messgeräte Einführungsverordnung, Fassung vom 24.03.2015“ and Requirements for Smart Meters Ordinance, 2011 – („Intelligente Messgeräte-Anforderungs-Verordnung“) [20]. According to these requirements, smart meters and their communication shall be secured and encrypted to avoid unauthorized access. Furthermore, communication needs to be authenticated and encrypted with individual customer specific key material.

Österreichs Energie released a requirements catalog which describes the minimum requirements for smart metering end-to-end security [21]. The catalog requires encrypted end-to-end communication between the end-user's smart meter and the utility's infrastructure.

CHAPTER 4

Functional Requirements for the Smart Grid Architecture

In order to draft the architecture of a smart hub system, it is important to define, besides the general requirements, the technical and technological requirements for cybersecurity, data privacy and security testing requirements. These requirements define various software and hardware specifications to ensure the security and privacy of stored and transmitted data and other functionalities like monitoring and regulating.

Based on the European standards, regulations, frameworks and recommendations, covered in chapter 3, the essential requirements have been extracted to build a smart hub system with a high security level.

The security requirements concerning cybersecurity, data privacy and security auditing can be clustered in the following categories (see the following subsections)

- Hardware requirements
- Software requirements
- Combined hard- and software requirements
- Cryptographic functionality
- Security testing and auditing technologies
- Privacy requirements

4.1 Hardware Requirements (HW)

For the cryptographic support of the smart grid system, a security module (for example a smartcard) is mandatory. The security module provides the trust anchor for many other security functions and specifically enables secure storage even with physical access by potential adversaries. On the outside of the smart hub, all components requiring cryptographically backed services, like authentication, integrity protection or encryption, must indirectly interact with the secure module.

4.2 Software Requirements (SW)

For connecting users, there must be security attributes like user identity, status of identity (if the user is authenticated or not), the connecting network, role membership and others. The user must authenticate, for example, with a password or a certificate, before any security relevant action can be taken. A proper developed ACL (access control list) is advisable to realize this standard. Furthermore, an access control policy must cover any operations between accessing parties (subject) and user data (object). It is also necessary that the smart hub can verify firmware updates for integrity and authenticity. A firmware update shall only be possible for administrative users.

Another important part of the smart hub are management functions. Those functions, such as reading version number, reading current time, firmware updates, deletion or modifications of events in logs, shall only be available for an authenticated user and defined role. In terms of data storage, validity check and integrity there must be precise rules for data. The received meter information shall be validated according to information security attributes, processing profile, time synchronization constraints (for instance, 3% deviation of measuring period), integrity, authenticity and confidentiality.

In addition, previous information content of a resource shall be made unavailable if no longer in use by any objects. Stored data shall be monitored for integrity and covered by action if a data integrity error is detected. Transmitted data shall be protected against accidental or malicious modification and be detected as such. This prevents falsified data to be transmitted.

Replay detection and reliable time stamps should also be implemented.

4.3 Hard- and Software (COMB)

The smart hub must provide a self testing suite and has to contain protection capabilities. The self testing suite should be running on initial start-up, at request and periodically during normal operation. A passive and/or active detection of a physical and/or logical attack shall be provided to verify the physical integrity.

To reduce the potential attack surface of the smart grid, only services needed for the specific action shall be exposed on the corresponding interface. Any functionality that is

not necessary must be deactivated, or it must be possible for the operator to deactivate it. Reducing the attack surface within the smart hub solution may be done on deployment and is a specialized task. It may be accessed by a small group of actors outside the solution. Therefore, it corresponds to the communication services, for example, for cloud services, web-services and internal/external services.

Additionally, the developer must ensure that the design of the devices takes into account the future proofness of the security functionality. As a result, the hard and software implementation should hold enough resources to be upgradable to newer, more resource-demanding security algorithms.

4.4 Security testing and auditing technologies (AU)

A requirement of the smart hub is to provide and protect audit capabilities, more precisely the log data should be provided and protected against tampering. This implementation is mandatory in the architecture of a smart hub. Furthermore, for defined events an alarm and audit log entry shall be generated to inform about critical events.

4.5 Cryptographic functionality (CRY)

To create a well constructed architecture for a smart grid, state-of-the-art crypto algorithms shall be used. All components of the smart hub must adhere to these specifications for a successful communication. The cryptographic suite should feature the following standards and functionality:

- ECC-Key pairs generation
- Diffie-Hellman key agreement (TLS)
- ElGamal key agreement (content encryption)
- PACE (Password Authenticated Connection Establishment)
- Signature generation and verification
- Import of public keys
- Secure messaging (AES CBC, AES-CMAC)
- Random number generation

The cryptographic primitives like key material, certificates, random numbers are sensitive material and must be generated using sufficient entropy and be protected against unauthorized disclosure at all times. Possible obsolete cryptographic data must be properly destroyed.

The smart hub must be able to use a public key infrastructure to detect and verify the identity of communication peers within the system. All needed certificates shall be generated and accessed with the secure module.

Another important requirement of the smart hub is to ensure end-to-end security and provide secure channel capabilities. The hardware security module must be used as a secure random number source, for TLS handshakes, signature verification and generation. The transmitted data in the smart system must be protected against eavesdropping and modification.

The data authenticity within the smart grid system must be guaranteed. Therefore, communication data shall possess a signature to verify the origin and sender of the data.

4.6 Privacy requirements (PR)

Regarding user privacy, it shall be enforced that no personally identifiable information can be obtained by an analysis of the communication data characteristics. Further, pseudonymity shall be provided for data which is not billing relevant or a secure operation.

The same standard applies to personally identifiable stored information such as measurements or log data. Data which is no longer needed should be safely and successfully removed from the system.

CHAPTER 5

Implementation of a Smart Hub

To combine the requirements for a smart hub system, listed in chapter 4, an application must be developed to integrate the desired functionality on a stand-alone device. The application itself takes care of security, energy management, alarm management and communication with third parties like weather forecast services and tariff information providers. Furthermore, a web interface should be provided to enable the user (typically the occupants of the building) to control their smart home.

5.1 Cybersecurity Architecture

Energy consumption and private usage data is sensitive information. In order to protect this information, several security measures to protect the privacy of the user must be implemented. A device that can switch relatively high loads can be a danger to the safety of the grid, especially if a vulnerability can be exploited on many devices at once, causing a spike load on the grid (see section 1.2.1). Therefore, operational security is just as important as protecting the users privacy.

A security module shall be developed for the smart hub solution to help with these tasks. It relies heavily on a Hardware Security Module (HSM) that stores the key material used to protect the platform. This shields the most vulnerable part of the solution, key storage. With this module, data and communication can be signed/verified and de/encrypted. This way the core principles of information security (confidentiality, integrity and authenticity) can be provided.

To secure the platform and application itself, a Secure Development Lifecycle (see chapter 2) shall be followed.

A potential architecture of a smart hub system, considering the regulations and requirements laid out in the previous chapters, has been developed and is visible in figure 5.1.

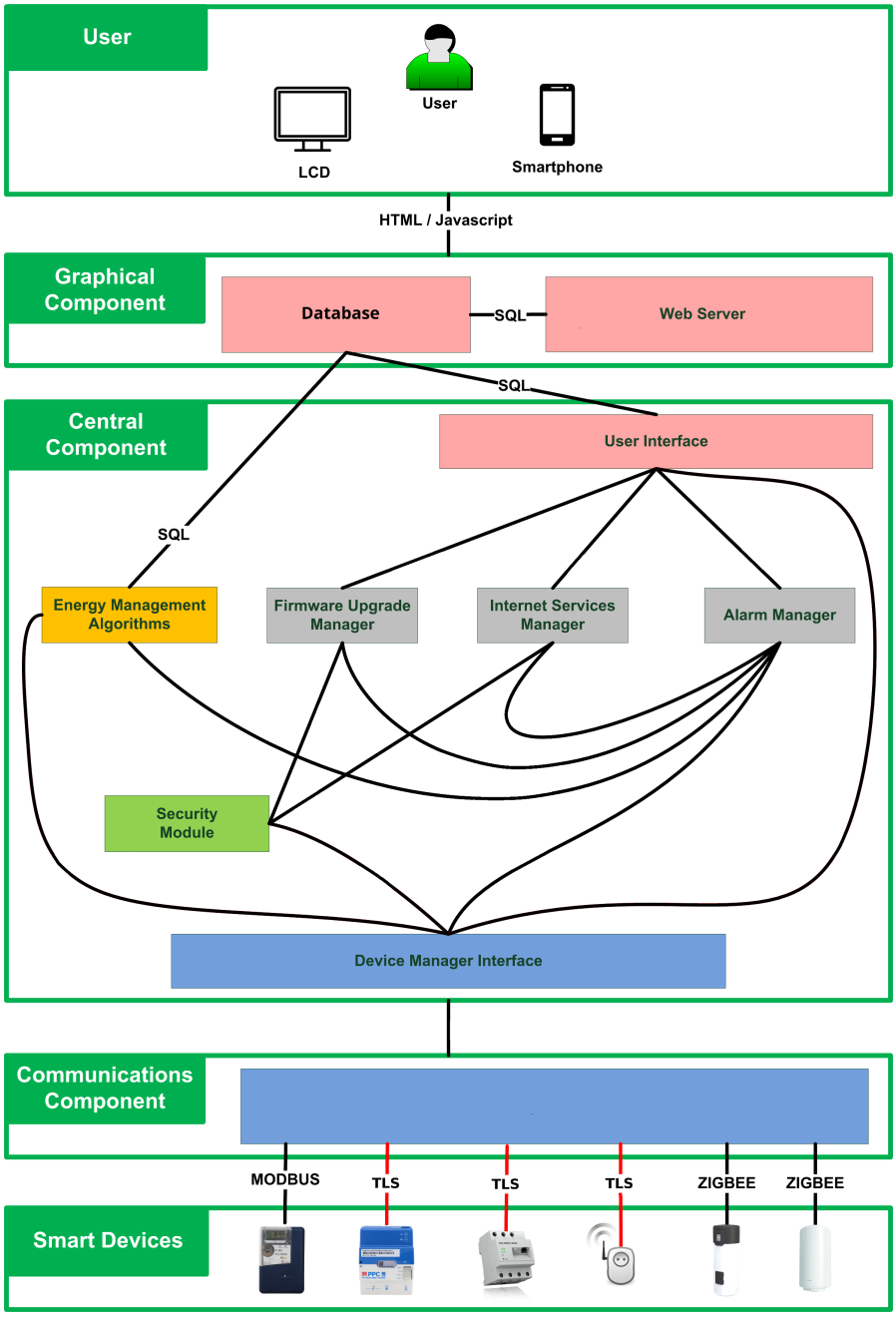

Figure 5.1: Example Software Architecture

It comprises the following components: the user, a graphical component (GUI), a central component, smart device communications components, and the smart devices. The components are described in the following.

5.1.1 User

The user can interact with the smart hub solution via a web interface. All user communication is protected with Transport Layer Security (TLS) protocol to ensure the privacy as well as confidentiality, integrity and authenticity of any user interaction and data.

5.1.2 Graphical Component

The graphical component provides the user interface via a webserver to remote users. The connection is to be secured with TLS. The web application on the server is connected to an internal database which provides synchronization and interaction with the core components and connected smart devices including security functions such as user authentication and authorization/permission checks.

5.1.3 Central Component

The central component contains energy management components, firmware upgrades, Internet services and alarm management services that interact with the user and device interface.

It comprises of an application based on a well-established framework to ease development, and optionally a local user interface with a touch display. The native application interacts with the database (over well defined SQL interfaces), the local user interface (touch display) as well as with the framework of the smart hub (Device Manager Interface with local REST API). The security module provides essential security function such as key and password storage, authentication or authorization checks and random number generation.

The security module uses a Hardware Security Module (HSM) that is described in more detail in section 5.2.

5.1.4 Communications Component

The communications component provides an abstraction layer between smart devices and the central component. Smart devices may utilize a number of different communication protocols, interfaces and technologies. These must be implemented in the communication component. Security functions such as protocol and technology specific authentication, encryption and integrity protection must be implemented whenever possible.

For instance, wireless ZigBee devices support secure communication, while on the other hand, wired Modbus devices typically do not support secure communication by themselves and thus no support for secure communication can be provided by the smart hub.

5.1.5 Smart Devices

The lowest layer of the grid system are the connected smart components. These components may utilize a wide range of different communication technologies and protocols that are abstracted through the communications component.

5.2 Hardware Security Module

A Hardware Security Module (HSM) is an internal or external device which is tasked with protecting sensitive information against an attacker.

There are two general concepts to provide such functionality:

- To provide a safe storage for the data itself on the HSM, by encapsulating and hardening the access, physically as well as through the digital interface
- To store key material on the HSM, which is then used to perform encryption and signature operations on data residing on regular storage

Since the smart hub system produces large volumes of historical meter data, the second solution is more appropriate, as cheaper mass storage can be used to store the meter data.

For the Hardware Security Module, several options are possible to use for the smart hub in accordance with smart grid requirements:

- SmartCard Based Modules
  - OpenPGP card [22]
  - YubiKey [23]
- Trusted Platform Modules

The smartcard based modules are built for highest hardware security. They employ chip design features that make it very hard to obtain key material by intrusive or side-channel attacks. Furthermore, it is a well-tested standard that is widely used in many security-critical sectors like finance and authentication systems.

OpenPGP is a cryptographic standard that is widely supported and provides open-source, well tested implementations for the GNU/Linux platforms. A dedicated smartcard is cheaper, but needs a smartcard-reader on the device. A Yubikey on the other hand is also a smartcard but has the reader included in a USB keyfob style. The cost of a smartcard reader is negligible in mass production, but can be substituted by a USB smartcard device for early development.

Trusted Platform Modules, on the other hand, behave like smartcards in many aspects, but are usually bound to a specific hardware. This means that a user would not be able to switch out a defective device and keep the cryptographic key. Furthermore, not all Trusted Platform Modules are supported on every possible operating system.

Following this analysis, a smartcard reader for OpenPGP smartcards was found to be the best option for the smart hub solution. Its reliance on well-tested open source software, low cost for mass production but also low development and engineering overhead for the development phase make it the ideal choice for a platform. The interface is standardized and also well supported in GNU/Linux systems, so swapping between a cheap on-board smartcard reader and the YubiKey (connected via USB) is seamless and requires no extra development. Furthermore, an exchangeable hardware security module can be bound to a specific user, eliminating the need to register devices before sending them to the user in case of a replacement. The user can just switch their smartcard to the new device and seamlessly continue to use the device.

5.3 Remote Access

To assist the user in case a problem occurs with their device, the smart hub platform can be accessed remotely. To prevent an attacker from exploiting this possibility, there are two mechanisms proposed:

First, the user must actively turn on the functionality, and sets a time for how long the connection is open. This decreases the attack surface greatly, as an attacker can only exploit flaws in the remote tunnel functionality if the user activated it for support purposes.

Secondly, the platform does not open an SSH server itself, but connects to a maintenance server over an SSH connection using public key authentication with the keys on the Hardware Security Module for authentication. This functionality (called reverse SSH tunnel) allows a maintenance connection while still keeping the attack surface low.

5.4 Platform Hardening

In order to shield the platform, the first layer of protection is reducing the attack surface. The attack surface denotes all services and ports reachable by an attacker on any interface.

A smart hub typically operates on an embedded system that runs an operating system. These operating systems provide high-level abstraction to the complex hardware to make implementation easier. A typical operating system for embedded systems is Linux.

Operating systems are often providing general network services in the default configuration. All services that are not needed for the functioning of the smart hub constitute an unnecessary risk of exploitation by an attacker.

It is therefore necessary to close or shut down all OS functionality that is not essential for the functioning of the smart hub.

Furthermore, if the operating system provides a firewall, the developers should make use of it and protect the smart hub from the outside world. Another hardening method that is often overlooked in embedded devices is keeping the system up to date by installing patches and updates that are released for the operating system.

5.5 Communication

The provision of cybersecurity is to be considered inside of the platform's central software components as well as in the communication with external entities.

External communication is between the hub and two separate areas: the WAN and LAN side of the network. While the WAN side can be considered more dangerous in terms of attacks, the LAN side must not be neglected as in today's world of "Internet of Things" other devices on the local network could be corrupted and used as an entry point to attack other devices on the same network.

For communication, reducing the attack surface means only running services essential to the functionality of the system. Furthermore, the services running should only offer trusted, up to date algorithms, protocols and cryptographic suites. This hardening of the operating system is to be performed in an initial step to secure the smart hub.

Communication on the WAN side of the device is protected by the Transport Layer Security (TLS) protocol, employing public key infrastructure to guarantee the identity of the communication partners.

For the LAN side, the communication of smart devices is often not in the control of the customer that bought said devices. This means that not all communication and control can be transmitted in a secure fashion. Nevertheless, the most secure method offered by a device is chosen to communicate with it, and data received from devices is validated for plausibility in order to prevent attackers changing the energy management via manufactured sensor readings.

5.6 Storage

Storage of user-specific data, mainly consumption data with a high resolution, needs to be protected from an attacker. This can be achieved by encrypting stored data with the key material from the hardware security module. Furthermore, data that is to be stored off-site (e.g. cloud, service provider infrastructure) should be transmitted encrypted and stored on the server pseudonymized or anonymized, depending on the usage of this data.

5.7 Firmware and Firmware Update

The firmware of the device must be protected against tampering by an attacker with physical access or access to the firmware update server. To achieve this, the firmware should be signed with the manufacturer's key so that an unauthorized change on the firmware can be detected before running it. For Linux systems, signed firmware update functionality is already a core feature that is provided by the platform.

5.8 Tamper Proofing

An attacker that has physical access to the device has more options than a remote attacker. The persistent storage and firmware of the smart hub can - without sufficient countermeasures - be accessed and manipulated. Two countermeasures are available to the system designer: encrypting and signing of the code base; detect tampering and making the violation known to the user.

Tampering can be detected using switches or other detection mechanisms on the casing of the device, indicating that it has been opened. This gives the user the opportunity to deal with the situation, for example doing a factory reset or a more sophisticated recovery mechanism provided by the smart hub.

5.9 Data Privacy Concept

To protect the user's data, both in transit and on the device itself, several measures need to be taken.

The data stored on the device is encrypted using the cryptographic functionality provided by the Hardware Security Module. Data in transit is only transmitted over TLS secured channels, and not stored on the remote end if not needed (data frugality). Also, remote endpoints need to authenticate themselves to prevent man-in-the-middle attacks.

5.10 Security Auditing Solutions

To test and verify the system before release, several standard measures are available to audit the platform. A certification according to Common Criteria should be sought after by the developers of the smart hub. For the application, a code audit should be performed to discover vulnerabilities and bugs that could be exploited by an attacker. Furthermore, the system can be analyzed in a penetration test to find flaws that occur in combination of the components.

5.11 Access Control List

To manage access control, a suitable system must be in place where all actions by a subject (e.g. user) on an object (e.g. historical meter data) can be allowed or denied.

This requires authentication of the user by password or certificate. For certain operations, the operating systems built-in mechanisms can be used to this end.

CHAPTER 6

Conclusion

In this work[1], a guide for the development of a secure smart hub was presented, with the aim to help developers avoid common mistakes that might lead to a number of risks for the owner of the smart hub.

First, an overview of the current smart home ecosystem was provided and possible repercussions of insecure smart home systems and smart grid devices were explained. A suitable tool for keeping security in mind during the process of development, the Secure Development Lifecycle, was suggested.

Further, an up-to-date summary of EU-wide and member country specific recommendations and regulations for smart metering was presented. The analyzed regulations vary between mandatory for the EU and mere recommendations. Nevertheless, the strictest requirements were derived so that a smart device that follows the requirements can be deployed in any european country.

Following this, functional requirements for all development aspects of a smart hub were laid out in categories covering software, hardware, cryptographic functionality, testing and auditing, and privacy. These requirements were derived from the regulations summarized in chapter 3.

Finally, security and privacy designs for implementing a smart hub were presented. An example design for the system, an analysis of available hardware security modules and various best practises for the modules of the smart hub have been defined.

This document can be used as a guideline for the secure development of a modular, flexible and secure smart hub which fulfills the EU-wide and member country specific recommendations and regulations for smart metering.

[1]This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 646580.

List of Figures

Bibliography

[1] W. Kastner, M. Jung, and L. Krammer, "Future Trends in Smart Homes and Buildings", in *Industrial Communication Technology Handbook, Second Edition*, R. Zurawski, Ed., CRC Press, Inc., 2014, ch. 59.

[2] G. Lobaccaro, S. Carlucci, and E. Löfström, "A review of systems and technologies for smart homes and smart grids", *Energies*, vol. 9, no. 5, 2016, ISSN: 1996-1073. DOI: 10.3390/en9050348. [Online]. Available: http://www.mdpi.com/1996-1073/9/5/348.

[3] ZigBee Alliance. (2012). Document 053474r20: Zigbee specification, ZigBee Alliance.

[4] Z-Wave Alliance. (). About z-wave technology, Z-Wave Alliance, [Online]. Available: https://z-wavealliance.org/about_z-wave_technology/.

[5] KNX Association. (). What is knx?, KNX Association, [Online]. Available: https://www.knx.org/knx-en/knx/association/what-is-knx/.

[6] Enocean GmbH. (). Enocean radio technology, Enocean GmbH, [Online]. Available: https://www.enocean.com/en/technology/radio-technology/.

[7] W. Granzer, F. Praus, and W. Kastner, "Security in building automation systems", *IEEE Transactions on Industrial Electronics*, vol. 57, no. 11, pp. 3622–3630, 2010.

[8] U. Greveler, B. Justus, and D. Loehr, "Forensic content detection through power consumption", in *2012 IEEE International Conference on Communications (ICC)*, Jun. 2012, pp. 6759–6763. DOI: 10.1109/ICC.2012.6364822.

[9] A. Dabrowski, J. Ullrich, and E. Weippl, "Grid shock: Coordinated load-changing attacks on power grids", in *Annual Computer Security Applications Conference (ACSAC) 2017*, Dec. 2017.

[10] M. Hutle and M. Kammerstetter, "Chapter 4 - resilience against physical attacks", in *Smart Grid Security*, F. Skopik and P. Smith, Eds., Boston: Syngress, 2015, pp. 79–112, ISBN: 978-0-12-802122-4. DOI: https://doi.org/10.1016/B978-0-12-802122-4.00004-3. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128021224000043.

[11] ENISA, "Smart grid security recommendations", European Union Agency for Network and Information Security, Tech. Rep., 2012. [Online]. Available: https://www.enisa.europa.eu/publications/ENISA-smart-grid-security-recommendations.

[12] BSI-CC-PP-0073-2014, "Protection profile for the gateway of a smart metering system", Federal Office for Inforation Security, Protection Profile, 2014. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0073.html.

[13] Smart Meters Coordination Group, "Privacy and security approach – part i", CEN-CENELEC-ETSI, Tech. Rep., 2013. [Online]. Available: https://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartMeters/Pages/default.aspx.

[14] NISTIR 7628 Rev. 1, "Guidelines for smart grid cybersecurity", National Institute of Standards and Technology, Standard, 2014. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final.

[15] Common Criteria for Information Technology Security Evaluation. (), The Common Criteria Recognition Agreement Members, [Online]. Available: www.commoncriteriaportal.org.

[16] ENISA, "Smart grid security recommendations, annex ii: Security aspects of smart grid", European Union Agency for Network and Information Security, Tech. Rep., 2012. [Online]. Available: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf/view.

[17] ——, "Smart grid security recommendations, annex iv: Smart grid security related standards guidelines and regulatory documents", European Union Agency for Network and Information Security, Tech. Rep., 2012. [Online]. Available: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/smart-grid-security-related-standards-guidelines-and-regulatory-documents/view.

[18] BSI-CC-PP-0077-V2-2015, "Protection profile for the gateway of a smart metering system", Federal Office for Inforation Security, Protection Profile, 2015. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0077+V2.html.

[19] BSI TR-03109, "Technische vorgaben für intelligente messsysteme und deren sicherer betrieb", Federal Office for Inforation Security, Technical Guideline, 2015. [Online]. Available: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/index_htm.html.

[20] E-Control. (2011). Intelligente messgeräte-anforderungs-verordnung, [Online]. Available: https://www.e-control.at/documents/20903/-/-/20a992e6-d11f-48b8-aef9-8e5d66f284c1.

[21] European Network for Cyber Security, “End-to-end security for smart metering”, Österreichs Energie, Requirements Catalog, 2018. [Online]. Available: https://oesterreichsenergie.at/files/Downloads%20Netze/E2E-Sicherheit-Anforderungskatalog-EN_1.1_final.pdf.

[22] OpenPGP. (). Card specification, [Online]. Available: www.g10code.com/p-card.html.

[23] yubico. (). Yubikey openpgp support, [Online]. Available: https://support.yubico.com/support/solutions/articles/15000006420-using-your-yubikey-with-openpgp.