Smart Grid Cyber Security: A German Perspective

Michael Wagner, Matthias Kuba, Andreas Oeder
Networked Systems and Applications Department
Fraunhofer Institute for Integrated Circuits
Nuremberg, Germany
Email: {michael.wagner, matthias kuba, andreas.oeder}@iis.fraunhofer.de

***Abstract*—Cyber security is an important issue in modern smart grid technology. As the smart grid is literally a network of networks, manifold potential vulnerabilities appear that allow privacy- and security-attacks within the whole energy chain, e.g. generation, transmission, distribution and consumption. Therefore, in order to achieve full customer acceptance and to ensure the stability of the current supply, all components of a smart grid communication network have to be highly secure and meet challenging privacy requirements. Scores of scientific and governmental efforts exist to make smart grid technology secure with respect to potential cyber-attacks. Nevertheless, standardization is mandatory to ensure sophisticated security mechanisms through the whole network. This paper focuses on the work of smart grid security aspects on the low voltage segment within the German power grid. Evolving security standards are discussed against the background of potential vulnerabilities and it is emphasized, where additional effort is necessary to ensure privacy and security in the smart grid.**

I. Introduction

Smart grid technology aims to increase the amount of renewable energy within the whole energy supply chain and to ensure reliable energy generation, transmission and distribution. Due to the distributed nature of the renewable energy sources, information and communication technology (ICT) is needed to interconnect decentralized generators and consumers. It is foreseeable that at least major parts of the backhaul communication on the low voltage segment will be IP-based. Therefore, numerous potential vulnerabilities to cyber-attacks arise. A list of cyber-attacks in the recent past on electricity generation-, transmission- and distribution-systems can be found in [1], including documented hacks and worm attacks on nuclear power plants, power plant safety monitoring systems, utility electronic control systems and commercial smart meters. Additionally, the US Federal Bureau of Investigation (FBI) reported smart meter hacks that might have cost a single electric utility hundreds of millions of USD annually over the last couple of years [2]. Consequently, cyber security is one of the most challenging issues for an evolving smart grid. In order to make the entire smart grid communication infrastructure safe against cyber-attacks, it is necessary to include cyber security mechanisms in all critical and vulnerable points and interfaces within the whole network. As the infrastructure and topology for smart grid based communication technology is not yet standardized, this is actually a very difficult task. Reams of publications can be found dealing with different aspects of smart grid security. A good overview is given in [3] and [4].

Several organizations work on the different aspects of smart grid cyber security all around the globe. In Germany, the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) is in charge of the smart grid's security aspects, focusing on a so-called smart meter gateway (SMGW). This paper introduces and evaluates the German efforts concerning smart grid security towards the SMGW. Firstly, potential vulnerabilities that pose a realistic threat on privacy, security and to some extent safety are exemplified. Subsequently, the proposals of the BSI with respect to the smart metering gateway security are introduced and discussed considering the background of the presented threats. Finally, conclusions are drawn, highlighting the advantages and drawbacks of the German approach.

II. Potential Vulnerabilities of Smart Grid Communication Architectures

The threats to the smart grid can be divided into three major scenarios: Manipulation, sabotage, and espionage. Manipulation can be accomplished at several system levels. Only technical manipulation will be discussed here, where the goal of the manipulator is to influence the process of mainly metering and billing via local modifications of the hardware or software. Obviously, the attacker needs to have direct access to the environment. Sabotage is not only a military scenario but also known as hacking of cyber-physical systems in the civil world. The aim is to find a weak point in the infrastructure and to gain control over controllable components. Accidents like a cable-cut caused by a digger can lead to comparable impacts. Direct access to the equipment is not necessary for those kinds of sabotage scenarios. Espionage is another class of threats within the smart grid, targeting at personal data like address, information about lifestyle, activities, absence times, domestic appliances or even bank account information.

The German work currently concentrates on the low voltage segment with a focal point on the SMGW. Even though manifold vulnerabilities are discussed in literature, the introduced three potential attack-scenarios seem to be the most relevant and realistic ones. Therefore we will focus on those major scenarios in this paper:

i. In a typical manipulation scenario, a software image which for instance is placed in the internet for free download could be installed to replace the existing software in the SMGW. It will cheat the distribution of the consumed energy towards the cheaper tariffs [2] or simply change

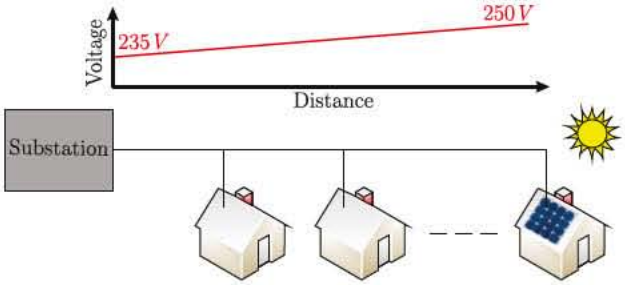

Fig. 1. Overvoltage caused by solar power system

the amount of energy metered. This attack is even easier to carry out for products based on open source software, since all the security mechanisms can be studied and altered in a dedicated way.

ii. The second threat, sabotage, is a destructive attack by actors from the internet. The aim is to gain control over controllable local systems (CLS) like photovoltaic plants, wind generators or combined heat and power stations. Switching many of them simultaneously can cause instabilities in the distribution network or even defects in electrical equipment - either in the smart grid itself, in the infrastructure, in buildings, plants or in a customer's home. A special attack of this kind can be done by preventing control over the local systems, e.g. by attacks to the infrastructure providing control information. With the following example, we show one of many possible scenarios which are prone for cyber-attacks: In some regions in Germany, the feed of solar energy may overload the existing low voltage distribution network. This may be a generic peak overload situation during noon of summer days with bright sunshine or a specific situation along the distribution line as shown in Fig. 1. The supply from solar power stations can cause overvoltage at the end of a line when the energy flows back to the transformer. Originally, the transformer was designed for feed-only scenarios, since energy recovery by the customer was not foreseen at that time. Therefore, the transformer is set up to supply an output voltage with a correct voltage level at the last consumer of the power line. Adding the voltage generated by the distributed energy generation systems to the transformer output without any adjustment-mechanisms may cause serious overvoltage. By means of a communication accompanying the smart grid infrastructure, the power feed can be controlled accordingly. Of course, blocking this control mechanism will cause trouble.

iii. The third threat, espionage, describes the illegal access to private or confidential customer information. This information can be used for precise energy consulting and billing, but it can also be misused in many ways. High time-resolution of the power consumption for example allows detection of the used equipment and its condition. From the type of equipment, conclusions about the room the equipment is located in can be drawn. Additionally, from the time distribution of switchable electrical equipment, the movement of the user can be deduced and the presence or absence of persons as well as the number of persons in a dwelling can be estimated. Concentrating this information in a central server forms a valuable target for privacy-attacks. Of course, similar insights into data from commercial customers would be valuable for interested parties.

III. German Approach for Secure Smart Grid Communication Architecture

In Germany, the BSI is in charge of the security-related aspects for the smart grid. It recently published a protection profile for a SMGW [5] and the preliminary technical guideline TR-03109 for SMGWs [6]. In this section, the security mechanisms defined by the TR-03109 guideline are described.

A. Protection Mechanisms Concerning the WAN Interface

According to the TR-03109 guideline, the SMGW hides the home area network (HAN) and the local metering network (LMN) behind a firewall, as shown in Fig. 2. The entire communication to the wide area network (WAN) can be initiated only by the SMGW. The only exception is a wakeup message from the (external) gateway administrator (GWA), prompting the SMGW to establish a connection between SMGW and the GWA. Due to this mechanism, connection establishment from external nodes is prohibited. In addition to this, the whole communication on the WAN is protected by transport layer security (TLS) [7].

B. Protection Mechanisms Concerning the HAN Interface

In the HAN, the user terminal and the CLS can address the SMGW. The CLS will be controlled from the WAN side. As the firewall prevents a direct communication between an external partner and the CLS, an SMGW proxy establishes two TLS communications - one to the CLS and another to an external partner. Hence, all CLS and external partners need a certificate from a certificate authority.

C. Protection Mechanisms Concerning the LMN

The SMGW has to support at least one RS485 communication interface and one wireless M-Bus interface. As stated in the current document, a TLS connection will run on top of TCP/IP over PPP over HDLC if the RS485 interface is used. Using the wireless M-Bus interface, the unidirectional communication enforces a simpler transport frame: the data is encrypted with AES-128 CBC and protected with a media authentication code (MAC) as described in [8].

D. Miscellaneous Mechanisms

Metering data is sent to the external market partners (EMP) via HTTP. The transferred data packet is intended to be routed by the GWA to the final destination - the EMP. Data packets which shall be routed by the GWA to an EMP must not only have a TLS encryption but also an additional end-to-end encryption to avoid unauthorized access to the data

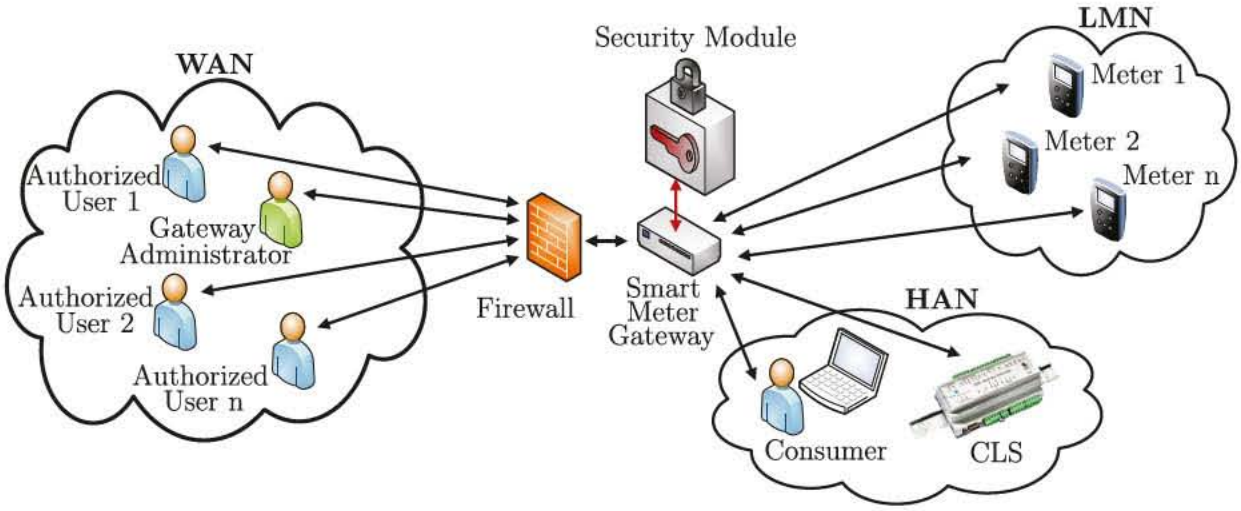

Fig. 2. Network architecture [6]

content by the GWA. In case of metering data, the data is end-to-end packaged into a cryptographic message syntax (CMS) formatted envelope [9]. The data is encrypted for the EMP, authenticated with the CMAC [8] and signed by the SMGW. The encryption and authentication keys are derived from an elliptic curve key agreement according to the ElGamal encryption system [7] from a key-pair specially generated for each envelope (ephemeral key) and the public key of the EMP. Net status data (voltage, phase, current) also can be sent in the same CMS format. To guarantee anonymity, a pseudonym is used for the internal addressing. As the signature is the only element that transports the identity of the SMGW, net status frames are always sent via the GWA to the EMP. The GWA replaces the signature of the SMGW with its own signature to ensure the anonymity of the customer.

The GWA is the only external participant that has access to the internal data structures of the SMGW like metering data, tariff conf guration, status information, logs and more via web services. These structures are represented as COSEM classes according to the companion specif cation for energy metering [10]. The SMGW holds three logs: the system log for status and error handling, the calibration log and the consumer log. The administrator has access to the f rst two but not to the customer log that holds all the data that are transferred to any instance, including the administrator himself. That way, the customer can control the administrator's actions.

The heart of the security concept of the German SMGW will be a security module containing the elliptic curve digital signature algorithm (ECDSA), the elliptic curve key agreement according to ElGamal (ECKA-EG), the key storage and the key generation. Initially, curves recommended by the National Institute of Standards and Technology (NIST) will be used. In 2015, brain pool curves shall be introduced, both based on 160 bit wide keys. The symmetric algorithms AES-128 and the secure hash algorithm SHA-256 are not covered by the security module but provided by the main system. The same applies to the message authentication code CMAC, which uses AES-128 encryption.

The TR-03109 also describes how the GWA keeps the data safe, starting with requirements concerning the architecture of the building and ending with the necessary audits for the administration team. This strict regulation is due to the almost unlimited access rights of the GWA. This means that the GWA has the most critical role in the communication process. The exact amount of SMGW-related information that is stored and needed by the administrator for the f rst-time operation and a fast replacement after a defect is still under discussion.

The SMGW is able to handle multiple tariff counters for each connected power meter and to send their values to an external partner periodically or on demand. On a local interface, a specialized terminal can offer measurement functionality. The consumer's personal computer as a human interface is not intended to be connected to the HAN. Its security status is currently unclear and connecting the HAN interface to a customer's LAN with direct internet access may bridge the f rewall by a direct connection to the WAN.

IV. Assessment and Efficiency of the Proposed Architecture

In the following, the resistance of the proposed communication architecture around the SMGW will be discussed against the three previously described classes of threats.

The threat of local manipulation is not taken too serious by the BSI. An anti-tamper seal as used for the meters of the last generation together with existing law and the assumption that a SMGW is installed in a non-public environment [5] is considered to be a suff cient inhibition threshold against local manipulation. State of the art security mechanisms like those used in cell phones or satellite radios could increase the robustness against local manipulation. These mechanisms allow strict control over the executed binary code. This usually works by booting from an internal ROM with disabled debug interface, loading the signed application image and testing the

signature before execution. Special controllers provide mechanisms to calculate the checksum of the image in the external RAM periodically and sense clock stops that are typical for RAM debugging. A security architecture that allows to hide internal boot-ROM, some RAM, some key fuses and relevant hardware interfaces in the application mode while disabling debug interfaces and program execution from external memory in secure mode makes system-designs possible that are hard to break.

The threat of sabotage caused by breaking into the smart meter gateway by network attacks seems to be impossible because of the specif ed authentication, encryption and access control mechanisms in [6] The only instance that has external access to the SMGW is the GWA. The f rewall functionality of the SMGW in combination with the requirement that outgoing encrypted communication establishment is only allowed by the SMGW results in a high protection level against attacks on the SMGW from the network side.

A realistic scenario for sabotage could be a denial of service (DOS) attack that can overload the communication infrastructure of the external partner, the network or the SMGW f rewall and therefore allow an additional attack scenario. When the communication between SMGW and GWA is blocked, the transmission of control information could also be blocked and as a result, the stability of the distribution network could be compromised. A possible counteraction against the impact of such DOS attacks could be a more decentralized control mechanism for energy generators (e.g. local voltage tracing and adaptive feeding of energy).

The specif ed mechanism in [6] concerning authentication, access control and encryption provides a high level of protection against unauthorized access to the SMGW. to The privacy mechanisms concerning locally stored conf dential information seem suff cient. In addition, the encryption of the communication (WAN and HAN) further increases the protection level. As a result, the espionage scenario exemplif ed by threat iii is suff ciently taken care of due to the described security mechanisms concerning the SMGW and the communication between SMGW, GWA and the user (user interface).

The GWA plays another important part within the whole scenario, since he is in charge of collecting, storing and distributing signif cantly conf dential data. Therefore, he could be prone to unauthorized data access and privacy attacks.

V. Conclusions

In this paper, several realistic vulnerabilities on communication technologies for the low voltage segment within the German power grid were presented. Furthermore, the work of the BSI concerning smart grid cyber security in Germany was introduced and discussed with respect to the potential attack scenarios. In conclusion, it can be emphasized that the security mechanisms proposed by the BSI concerning the SMGW with regard to unauthorized access are suff cient but the conf dential and private data kept by the GWA can be seen as potentially vulnerable.

The protection prof le [5] currently is in the process of certif cation. The TR-03109 is planned to be f nished in December 2012.

Acknowledgement

The work and contributions for the smart meter gateway def nitions have been funded through the Bavarian State Government as part of the project NET within the Energie Campus Nürnberg.

References

[1] A. R. Metke and R. L. Ekl, *Smart Grid Security Technology*, IEEE Conference on Innovative Smart Grid Technologies, 2010.

[2] KrebsOnSecurity Article, *FBI Smart Meter Hacks Likely to Spread*, Online: http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/, 2012.

[3] Y. Yan, Y. Qian, H. Sharif and D. Tipper, *A Survey on Cyber Security for Smart Grid Communications*, IEEE Communication Surveys & Tutorials, 2012.

[4] T. Baumeister, *Literature Review on Smart Grid Cyber Security*, Tech Report, 2010.

[5] Federal Off ce for Information Security, *Protection Prof le for the Gateway of a Smart Metering System - Gateway PP*, v01.01.01 (Final Draft), 2011.

[6] Federal Off ce for Information Security, *Preliminary Technical Guideline BSI TR-03109 - Smart Energy*, Version 0.50, 2012.

[7] E. Rescorla, *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*, Internet Engineering Task Force (IETF), RFC 5289, 2008.

[8] J. H. Song, J. Lee and T. Iwata, *The AES-CMAC Algorithm*, Internet Engineering Task Force (IETF), RFC 4493, 2006.

[9] R. Housley, *Cryptographic Message Syntax (CMS)*, Internet Engineering Task Force (IETF), RFC 3852, 2004.

[10] International Electrotechnical Commission, *IEC62056 Standards for Electricity Metering*, 2002.