International Journal of Smart Grid and Clean Energy

A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures

Florian Skopik[a]*, Zhendong Ma[a], Thomas Bleier[a], Helmut Grüneis[b]

[a] *AIT Austrian Institute of Technology, 2444 Seibersdorf, Austria*
[b] *Linz Strom GmbH, 4021 Linz, Austria*

Abstract

The smart grid initiative aims at transforming today's public power grid into a flexible and intelligent energy utility. The basis for this advancement is the detailed monitoring of the grid status and energy consumption behavior of connected stakeholders in order to implement powerful control mechanisms, flexible billing processes, and unmatched value-added services. However, these advantages do not come without costs. System components grow in complexity and increasing integration of power grid control systems with information and communication technology (ICT) leads to novel security and privacy challenges. Therefore, this paper deals with a structured analysis of vulnerabilities and threats that have the potential to hinder the functioning and wide adoption of automatic metering in smart grids. This analysis provides valuable input for further specification and development of critical system components and security and privacy protection mechanisms.

Keywords: Smart grid security, smart metering, threat survey, attack vectors, countermeasures

1. Introduction

The smart grid [1] [2] promises numerous advantages compared to today's grid technology, including automatic meter reading and billing, dynamic pricing, detection of impending black outs, and flexible feedback of privately produced energy. By effectively transforming today's public power grid into a smart grid, novel system features are introduced, such as fine-grained monitoring, two-way communication services, and online energy profile management. A key factor to achieve these ambitious goals is the comprehensive roll-out of smart meters and the construction of a reliable smart metering infrastructure. However, implementing such a complex infrastructure is challenging due to (i) technological diversity of devices ranging from microcontroller technologies to large-scale communication networks; (ii) vertical security mechanisms consistently spanning all architectural layer; and (iii) long-term operability of equipment and robustness against future threats.

Since the electric power supply is one of the most critical infrastructure services today, comprehensive and advanced security and privacy mechanisms are needed to guarantee smooth and reliable operation of the smart grid and to cope with today's security challenges. In particular, massively produced amounts of data need to be carefully protected against misuse. Numerous security mechanisms need to be incorporated in the design of this infrastructure to gain customer trust and ensure a wide adoption of this new technology. A thorough analysis of technical vulnerabilities and identification of threats is an important step toward securing smart grid infrastructures and the basis for developing advanced security and privacy protection mechanisms.

Therefore, in this paper we provide a structured analysis on vulnerabilities and threats related to smart grids. Because the smart metering infrastructure is envisioned to be a rather open system to allow access from various devices and users, our focus is on the issues related to smart metering infrastructure. Our

* Manuscript received July 13, 2012; revised August 13, 2012.

Corresponding author. Tel.: +43-664 8251495; fax: +43-50550 2813; *E-mail address*: florian.skopik@ait.ac.at .

main contributions are as follows:

- *Smart Grid Security Principles.* We highlight a typical smart grid structure, show potential attack targets in the whole system, and outline attack incentives, and methods.
- *Report on Major Vulnerabilities and Threats.* The main part of the paper deals with a systematic analysis of actual threats and potential weaknesses in today's smart meters and utilized network technologies.
- *Survey on Threat Countermeasures.* Based on an analysis, here, we report the highlights of an in-depth survey on appropriate countermeasures to the discovered threats.

The remainder of the paper is organized as follows. Section 2 outlines a basic smart metering infrastructure and key principles of information security. The following Section 3 summarizes vulnerabilities of smart meters and applicable countermeasures to potential attacks. A similar view on risks concerning the utility company's data centers is provided in Section 4; while Section 5 discusses threats and data privacy concerns, especially for future Web-based community applications on top of the smart grid. Finally, Section 6 concludes the paper.

2. Smart Grid Security Principles

2.1. Entities in smart metering infrastructures

We divide our analysis on security threats in the smart metering infrastructures according to a hierarchical structure. Here, major entities and their connecting networks are separated in a layered model: (i) *Intelligent Electric Appliances:* are connected through a local home area network (HAN) to the smart meter in order to report detailed energy consumption data, but also to be controlled by the smart meter and utility company respectively based on dynamic price models. (ii) *Smart Meters:* measure the total power consumption and (optionally) collect the consumption of single devices. Data is reported to the next concentrator node through a neighborhood area network (NAN). (iii) *Concentrator Nodes:* monitor and collect data from several smart meters in proximity. More intelligent devices can preprocess and compress this data which is pushed to one or several data centers via a high-speed backhaul (WAN). (iv) *Utility Data Centers:* store and process received data used for accounting and billing (even by third parties), but also for monitoring and actively controlling the power grid status. (v) *Web Platforms:* People may use value-added applications to monitor and manage their energy consumption behavior online.

In this paper, we structure the analysis on threats and vulnerabilities in three tiers:

- **Tier 1:** deals with threats to electric appliances, smart meters and their uplink to concentrator nodes. This part is often referred to as the 'last mile' and is considered as most vulnerable to attacks due to the physical accessibility of devices.
- **Tier 2:** deals with vulnerabilities of the uplink from smart meters over concentrator nodes to data centers and interfaces to Web-based applications.
- **Tier 3:** deals with Web-based applications and value-added services that use gathered meter data.

2.2. Key principles of information security

Security-sensitive topics [3] are typically discussed in context of the so called CIA triangle: *confidentiality*, *integrity*, and *availability*. Metering services are essential to ensure reliable energy provisioning, and meter readings are highly sensitive data whose protection is a major objective in future infrastructures. Therefore, we follow the same approach, and further outline fundamental areas of smart meter infrastructures with respect to these three pillars.

Confidentiality is concerned when it comes to creating, transferring, processing, and storing customer data, either dynamically produced data, such as meter readings and energy consumption profiles, or static data, including credit card information used by the energy provider to account for services. In today's information society, customer data is a highly important asset for every company, and the exploitation of user profiles has to be avoided by appropriate privacy preserving mechanisms.

Integrity of reported energy consumption data is of paramount importance since this information is used for accounting and billing. Numerous possible frauds need to be prevented, such as a customer sends tampered meter data in order to pay less; or make someone else to pay more. Thus, manipulation of the smart meter itself or injection of tampered messages in the network must be avoided (or at least detected and compensated). Furthermore, injecting wrong status messages in the communication network might cause problems in the net management, e.g., reporting overload messages might urge the utility company to reshape the power grid's structure.

Availability concerns are twofold: From a customer's perspective the availability of electricity is most vital; meaning, no one is able to turn off electricity accidentally or maliciously. From a utility company's perspective remote meter readings are essential to prevent energy theft and keep the business running. Furthermore, status messages delivered from smart meters can be used to actively reconfigure the grid in case of (temporally) unexpected load conditions. Thus, the availability of the smart meter communication is essential here.

2.3. Smart grid protection objectives

We identified the following objectives to be the most important ones to be protected in the future smart grid: (i) *Availability of the Power Grid.* This includes correct operation of energy generation, transmission, and distribution as in today's grid. However, besides physical attacks, numerous cyber-attacks are possible to interrupt correct operation, such as tampered control messages which may cause overloads or temporal blackouts. (ii) *Legitimate Power Consumption and Delivery.* The goals are, on the one side to prevent energy theft and ensure consistent measurement of obtained energy; on the other side the correct measurement of fed back energy in case of the integration of private solar panels and wind turbines. Transparent billing and accounting are evident to establish and maintain trust relations between consumers and producers. (iii) *Privacy of Consumers.* Secure power consumption data handling (including, transmission and storage) is of paramount importance, as well as privacy-aware profiling and mining of behavior patterns. The goal is to avoid the exploitation of real-time energy consumption monitoring mechanisms.

3. Tier 1: Smart Meter Vulnerabilities

Smart meter vulnerabilities are exploited by attacks to the smart meter (device) itself and/or its interfaces in several ways, either by (i) manipulating the hardware, (ii) manipulating the firmware, or (iii) exploiting limitations design and implementation.

3.1. Attack methods

3.1.1. Hardware manipulations

Current smart meters are designed to remain in a valid operating mode even if communication with the data center or concentrator node is lost. This is required to ensure smooth operation in case of unintentional communication disruptions. Thus shielding the antenna of a wireless module (e.g., WiFi 802.11 or ZigBee 802.15.4) or using an electric filter to suppress high frequencies of a modulated signal on the power line, is a first step to prevent remote meter readings. Furthermore, once a smart meter's housing has been successfully opened, there might arise opportunities ways to get access to the firmware; for instance through an unsecured ISP port or sophisticated lock bit attack methods [4]. Finally, exchanging devices between different locations, replacing smart meters with cloned devices, or at least their communication modules can lead to inaccurate accounting and billing.

3.1.2. Firmware manipulation

These attacks aim at modifying the intended program flow of the smart meter operating system, e.g., by interrupting the internal and external power supply, or exploitation of a local service port. Smart meter producers invest high effort to prevent such attacks, e.g., by checking the consistency of meter readings or sending a 'heart beat' signal in periodic time intervals. However, also reprogramming the actual firmware located in the smart meter's flash memory is possible by skilled attackers having insider knowledge.

3.1.3. Exploiting limitations of design and implementation

Although many sound security concepts exist and a system may be securely designed (at an appropriate level), usually some conditions are not sufficiently considered and failures are made in the actual implementation, for instance transmission of encryption keys over unencrypted channels [5].

3.2. Countermeasures and obstacles

3.2.1. Authentication and strong encryption of communication

An obvious requirement is proper authentication of devices and encryption of communication to avoid eavesdropping and sending tampered messages. This countermeasure to numerous attacks does not only concern communication in the HAN and NAN, but also buses within smart meters.

Obstacles (i) Microcontrollers need to be cheap and simple from an economic point of view; but powerful to handle strong encryption methods from a security point of view. However, when a low cost is of priority, security suffers. (ii) Keys need to be changed periodically, especially if they have been discovered. However, updating keys in a potentially broken symmetric encryption system is a non-trivial task. (iii) On small devices, weak implementations of pseudo-random number generators (PRNG) with bad statistical properties deliver values that are predictable to a certain extent. This poses a basic vulnerability if used by encryption modules. (iv) Numerous weak implementations and so-called closed industry standards are used in near field radio communication (HAN) where well-tested and wide-spread technologies (such as IP-based products) are often not used due to power consumption restrictions.

3.2.2. Secure key management

Encryption Keys are the most critical part to ensure secure operation of the automatic meter infrastructure (AMI) [6]. Various obstacles however burden the wide adoption of appropriate key management.

Obstacles. (i) Individual key management is technically complex and expensive for the large number of deployed devices. Furthermore, keys within the machine need proper protection to avoid their disclosure through side channel attacks [7]. (ii) Complex architectures which include smart meters, concentrator nodes and utility backend servers require seamless key management across all layers. (iv) Secure remote key distribution in symmetric encryption systems is challenging, however PKI requires higher computational performance and thus more expensive devices. (iv) Social engineering is a major threat here, since a large amount of people will be involved in deploying and servicing the whole infrastructure.

3.2.3. Securing the firmware

The firmware of the device controls the actual mode of operation and implements energy measurement, event logging and reporting to the utility company. The smart meter firmware must be secured from manipulation. Even reading the firmware could disclose information which could be used for attacks, e.g., pre-programmed keys.

Obstacles. (i) Some recent blog entries [8] claim that even simplest security methods are sometimes not applied in today’s devices (such as programming the lock bit to avoid firmware readouts). (ii) There were even reported attacks (e.g., against the lock bit of common microcontrollers) used to read back an actually secured firmware [4] [9]. One solution to this problem is to use secure flash memories that encrypt the program code itself, which however, require a powerful CPU to decrypt on the fly (tradeoff between price and performance, but as well power consumption).

3.2.4. Secure source code development

A security-focused firmware development cycle, including frequent walkthroughs and security assessments by either third parties or at least people different from the developer team, are an effective means to discover bad design decisions and implementation flaws.

Obstacles. (i) Various tools and methods are available for static code analysis, e.g., Secure Programming Lint, but are rarely used even when developing components for critical infrastructures due to increasing costs and development time. (ii) External assessments are often skipped because of protected intellectual properties. (iii) Penetration testers frequently underestimate the community’s innovation regarding the development of new hacking methods.

4. Tier 2: Utility Vulnerabilities

The electric utility topology can be physically shaped in several ways [10]. However, here, more important is the (logic) topology of the communication overlay network, used to request readings from the smart meters. Two fundamental approaches are broadly discussed here. First, a meshed NAN network connects smart meters in a peer-to-peer fashion, thus even devices in different houses can communicate with each other. This model foresees neighboring devices as relays if no direct uplink to a concentrator node is available. This model is often assumed when assessing smart grid security, since it would easily enable viruses and worms to spread, and thus a vast field of potential attack strategies. But actually, second, strictly hierarchical topologies are more likely to be implemented, where a meter can report to only one predefined concentrator node and avoids direct communication with other meters.

4.1. Attack methods

4.1.1. NAN sniffing

The aim of NAN Sniffing is to break network encryption, disclose the communication protocol, and learn about data formats and grid status message types; ultimately, to capture another smart meter's reported consumption data (effectively enabling an attacker to create consumption profiles of foreign households) and to send tampered messages to the data backend. The success of eavesdropping depends on topology and technology of the infrastructure (e.g., dedicated channel or shared IP channel etc.). Apart from consumption profiling, NAN sniffing would be the first step in a multi-staged attack and thus, the basis for active manipulation of own or foreign meters.

4.1.2. Own or foreign meter emulation

Once the NAN protocols and message formats have been discovered and properly reverse engineered respectively (using methods discussed before in context of Tier 1), one could potentially emulate his own smart meter in order to send tampered consumption data to the next concentrator node. This would enable at least energy theft. However, with significantly more effort, one could also be able to spoof a foreign meter; for instance, through key sniffing on the NAN. Depending on deployed authentication mechanisms, further attacks would deal with active message spoofing, e.g., to cause a victim higher electricity bills.

4.1.3. Large-scale meter takeover

Recently, [11] demonstrated the possibility of spreading worms in a smart grid with a peer-2-peer topology. This would effectively allow an attacker to take over a larger amount of smart meters similar to Internet worms which install backdoors on PCs. Controlling a large-scale ‘smart meter botnet’ [12] would enable attackers to cause wide-range harm. For instance, sending coordinated fabricated grid overload status messages from numerous devices could prompt the utility to shut down certain segments of the grid to avoid local overloads. In another scenario, forcing thousands of smart meters to turn off and on simultaneously could cause major trouble due to quickly changing load conditions on the power grid.

4.1.4. Concentrator node(s) attacking

Detailed attack strategies highly depend on the employed technologies in the concentrator nodes, but they are in general similar to methods described in the sections before (i.e., eavesdropping, reverse engineering, message tampering, denial-of-service). However, a larger amount of grid users is concerned, if a concentrator node is compromised and its normal mode of operation disrupted.

4.2. Countermeasures

Various countermeasures ease the effect of presented attack strategies. Notice that due to diversity of technical approaches, legal objectives, and network technologies, this section can only provide a rough overview.

4.2.1. Secure system design

As applicable to all other critical systems, secure design is the most important preventive *countermeasure* against most attacks. A system that has been thoroughly designed and reviewed by the means of penetration testing and third party assessments is absolutely essential for a critical infrastructure such as the power grid. Secure system design refers, for instance, to a hierarchical model with well-defined boundaries for each layer implementing individual protection mechanisms. It further includes well-proven authentication, authorization and encryption mechanisms. Moreover, in case of security breaches (e.g., pre-shared keys are disclosed), caused harm must be kept to a minimum. For that purpose a structure and design that allows for fast detection and recovery in case of attacks must be applied.

4.2.2. Secure operation

Security-aware operation includes the application of SCADA approaches, including online monitoring of network traffic (deduction of usual behavior), and detection of suspicious behavior (e.g., through threshold alerting when exceeding normal traffic levels deduced from historic monitoring data). Furthermore, similar to major pay tv security systems, there should be mechanisms to exclude tampered devices from the network on the next key or firmware update cycle. Besides these technical measures, security management spans several further aspects, such as personnel security (i.e., background checks of employees), and security assessments of organizational processes and management procedures. However, these aspects are out of scope of this paper.

4.2.3. Secure service evolution

Once installed smart grid components (smart meters, concentrator nodes) are planned to remain operational for decades. During this time considerable technical progress will require targeted updates in order to tackle discovered security holes and update inefficient security measures. To this end, most devices have the ability to receive remote firmware updates. However, realistically, limited computational power will most likely prevent long-term updateability; for example, new features (protocols, encryption) may have higher hardware requirements. Furthermore, there might emerge some new requirements that cannot be covered by software implementations but need hardware modifications and thus causing cost-intensive device replacements.

5. Tier 3: Web Application Vulnerabilities

The top tier deals with smart metering data management and value added services, including semi-automatic or even fully automatic billing and accounting. Since this is the most complex part of the smart metering infrastructures, a detailed threat analysis would require in depth analysis of deployed components. Therefore, we provide a basic overview which highlights threats on an abstract level only.

Basically, attacks on the Web application level will either aim at disrupting meter reading management services or stealing metering data in order to derive higher level information, such as individual consumption profiles. Thus, typical threats are not only the unavailability of services through (D) DoS attacks, but also threats to privacy through user behavior profiling. Aggregating and correlating smart meter readings allows the construction of detailed user profiles which is interesting information, for instance, for advertisement. It is essential to support the creation of trust relations between customers and utility providers by establishing transparent billing processes and traceable pricing, as well as informing customers about stored data (personally identifiable information). Nevertheless, appropriate countermeasures, such as anonymization and pseudonymization techniques for metering data [13] need to be employed to prevent misuse from the beginning. Notice, that the data backend will make use of a wide variety of standard server software and technology. Thus, this layer is generally vulnerable to all broadly applied server attacks against particular products and versions. Their discussion however is far beyond the scope of this paper.

6. Conclusion and Future Work

We like to conclude with a set of recommendations for risk mitigation. Derived from the analysis' findings, the design of future smart grid infrastructures need to be centered around: (i) Physical robustness and tamper resilience of smart meters and concentrator nodes; (ii) Authentication of users and devices using strong passwords, digital certificates and signatures; (iii) Authorization of users and devices to grant them least privileges to access resources and services. (iii) Encryption of communication data and user data in the utility data center; (iv) Integrity and plausibility checks of data, such as meter readings, grid status messages, and network traffic; (v) Training of technicians and service staff to prevent social engineering.

Discussions with the Austrian utility provider *Linz AG* revealed – besides the presented (ICT) attack vectors in this paper – that serious efforts are required in order to physically secure transformer stations and included concentrator nodes. While most smart meters are already designed to be largely resistant against a variety of physical attacks, e.g., through tamper-resistant housing etc., concentrator nodes, which are deployed in a usually controlled industrial environment, are not. Thus, once an attacker gains physical access to a transformer station a multitude of attacks on concentrators might be possible because of the potential coupling to the controlling SCADA backend (depending on the overall architecture). Combining physical security and cyber security measures in a consistent strategy is therefore a first priority – especially for future research initiatives.

Work in this paper is only the first – but an essential – step toward a secure smart grid. We focused only on the smart metering infrastructure. The smart grid however incorporates numerous additional aspects besides automatic meter readings; for instance, dealing with intelligent energy distribution or automatic controlling of overload scenarios. For that reason, numerous further challenges, as pointed out for instance in [14] [15], need to be addressed to evolve today’s power grid to a real *secure* smart utility.

Acknowledgements

This work received funding from the European Union through the FP7 project PRECYSE (285181).

References

[1] Massoud AS and Wollenberg BF. Toward a smart grid: power delivery for the 21st century. *IEEE Power and Energy Magazine*, 2005; 3(5)34–41.

[2] Tsoukalas LH and Gao R. From smart grids to an energy internet: Assumptions, architectures and requirements. In: *Proc. of Third International Conference on Electric Utility Deregulation and Restructuring and Power Technologies*, 2008:94–98.

[3] Anderson RJ., *Security Engineering - A Guide to Building Dependable Distributed Systems*, 2nd ed. Wiley, 2008.

[4] Carpenter M. Hacking AMI. (2008). [Online]. Available: http://inguardians.com/pubs/090202-SANS-SCADAHackingAMI.pdf

[5] Wright J. Killerbee: Practical zigbee exploitation framework. (2009). [Online]. Available: http://www.willhackforsushi.com/presentations/toorcon11-wright.pdf

[6] Metke AR and Ekl RL. Security technology for smart grid networks. *IEEE Transactions on Smart Grid*, 2010; 1(1):99–107.

[7] Goodspeed T. Breaking 802.15.4 AES128 by syringe. (2009). [Online]. Available: http://travisgoodspeed.blogspot.com/2009/03/breaking-802154-aes128-by-syringe.html

[8] Lawson N. Reverse-engineering a smart meter. (2010). [Online]. Available: http://rdist.root.org/2010/02/15/reverse-engineering-asmart-meter/

[9] Skorobogatov S. Semi-invasive attacks - a new approach to hardware security analysis. PhD dissertation, University of Cambridge, 2005.

[10] Flick T and Morehouse J. *Securing the Smart Grid: Next Generation Power Grid Security*. Syngress Media, 2010.

[11] Davis M. Smartgrid device security: Adventures in a new medium. Presented at: BlackHat Technical Security Conference, 2009.

[12] Abu Rajab M, Zarfoss J, Monrose F, and Terzis A. A multifaceted approach to understanding the botnet phenomenon. In: *IMC*. ACM, 2006:41–52.

[13] Efthymiou C and Kalogridis G. Smart grid privacy via anonymization of smart metering data. In: *Proc. of 2010 First IEEE International Conference on Smart Grid Communications*, 2010:238–243.

[14] Amin M. Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid. In: *Proc. of PES General Meeting,* 2008:1–5.

[15] Khurana H, Hadley M, Lu N, and Frincke DA. Smartgrid security issues. *IEEE Security & Privacy*, 2010; 8(1)81–85.