Smart Meters Security Assessment in the Brazilian Scenario

Rafael Cividanes, Nelson Uto, Bruno Botelho,
Sergio Ribeiro, Christiane Cuculo
Information Security Management
CPqD Foundation
Campinas, São Paulo, Brazil
{rafaelsc, uto, bpereira, sribeiro, ccuculo}@cpqd.com.br

Danilo Suiama, Heron Fontana
Management of Metering, Losses and Technology
ELEKTRO
Campinas, São Paulo, Brazil
{danilo.suiama, heron.fontana}@elektro.com.br

Abstract – Smart meters play an important role in smart grid architectures and technologies. Preliminary research has already indicated vulnerabilities as well as attacks likely to happen on the new meters. The Brazilian scenario combines two main perspectives: one is the growing rate of fraud in the electric energy measurement and the other is a resolution that establishes the replacement of all electromechanical meters with the new smart meters. This paper presents a threat modeling in smart meters and some possible attacks related to the mentioned scenario. It also discusses the ongoing Brazilian R&D project that focuses on security assessment of these new devices and the creation of a laboratory for smart meter vulnerability research and pentest execution.

Keywords-smart meter cyber-security; vulnerabilities; attacks; security laboratory for smart meter pentest

I. INTRODUCTION

The Smart Grid technology brings several benefits to the utilities, the customer and the environment, such as: increased resilience after service disruption, flexible distribution, energy efficiency (less waste), enhanced usage monitoring, variable pricing structure, reliability and operational efficiencies, renewable sources of energy, etc. However, these benefits come together with some security concerns, including many types of vulnerabilities related to each asset, system or communication channel in the Smart Grid architecture. In fact, each Smart Grid component can be the target of an attack: communications, meters, transmission substations, distribution substations, and corporate network. Each element should have integrity mechanisms working properly [1]. The Smart Grid security issue is being analyzed and some publications have been issued [2] [3].

The implementation of Smart Grids in Brazil has an important goal: the reduction of non-technical losses. In the current scenario, the energy theft in Brazil represents a loss of US$ 1.4 billion, not including taxes. For example, the city of Rio de Janeiro has about 20% of energy loss. The new electronic meters will help detect and reduce this huge loss. However, if not properly designed and tested, the use of these new meters may have a huge impact on the entire Advanced Metering Infrastructure (AMI).

Almost all residential and business customers (low voltage) in Brazil are using electromechanical energy meters and the fraud techniques related to these current meters are well known and even obsolete. Violations are restricted to physical attacks. On the other hand, the new electronic smart meters open the door for vulnerabilities to be exploited. Firmware analysis, data extraction, access to cryptographic keys, bus sniffing, denial of service, etc., are examples of actions that could be performed to compromise a smart meter device. In this case, not only physical but also logical attacks are feasible.

In August 2012, ANEEL (Brazilian Electricity Regulatory Agency) approved a resolution which states that energy distributors will have to install electronic meters for all consumers who choose to be billed in differentiated tariffs. It is the first step by the Brazilian Government to replace the 67 million electromechanical meters by January 2014. This is a unique moment in the history of the Brazilian energy sector when all meters will be replaced. However, the choice of smart meters with security weaknesses or severe vulnerabilities may cause serious damage to Brazilian economy.

It is in this context that the research and development Project entitled *Security Assessment for Smart Meters* was designed. The objective is to investigate different brands and types of smart meters available in the market, then run tests on them for checking security requirements, assess potential impacts, and finally build the Smart Meter Cyber Security Laboratory specialized in security evaluation of smart meters. The results will help the entire energy sector in Brazil and the development of additional security regulations and standards to be included to metrologically relevant requirements currently in use by Inmetro (Brazilian agency responsible for running tests on the meters).

The remaining part of this paper is structured as follows: Section II describes a threat modeling applied to smart meter devices, presenting what could be done if these assets were designed without considering a security baseline. Section III presents some possible attacks, how they are executed and the concepts related to the existing vulnerabilities. Section IV presents a synthesis of the Brazilian project, addressing the objectives, methodology of work, mechanisms of security tests and the establishment of a Laboratory. Finally, the conclusions are exposed in Section V.

II. THREAT ASSESSMENT IN SMART METERS

In the field of Smart Grid security, one of the most important components are the smart meter devices. They are the front door of several types of attacks on security. Besides being the common hub in the Smart Grid architecture, they are in the wild (outside the physical boundaries of the utility

ISBN: 978-1-61208-259-2

company's property), which increases the probability of vulnerability exploitation. The physical access to these devices, which can be easily obtained by consumers and adversaries, facilitates the execution of an attack. In order to study and understand the smart meters' characteristics and mechanisms of protection (if any), any individual can, for example, buy a device on eBay.

Smart meter devices are made of electronic components and encompass different types of technologies, protocols, and embedded systems. The risks related to these new devices come from the fact that they are, almost never, built with security requirements in mind. In this way, it is expected that they would fail if exposed to unexpected situations, creating opportunities for security violations. Thus, to mitigate these risks, it is essential to determine the attacker's perspective, which generally includes the opportunity for financial gain, the opportunity for mischief, and the opportunity for chaos [4]. These perspectives can result in different kinds of threats, depending on each country's scenario.

In the Brazilian scenario, it is possible to identify four main threats: (1) energy usage frauds; (2) user privacy violation; (3) propagation of malicious code to others meters through the AMI; and (4) malicious interruption of electricity supply. Each threat outlined above can result from different security vulnerabilities being exploited, culminating in success of the attack. However, in all the cases, the threats exist because of the smart meters' technological characteristics, i.e., the existence of a firmware (maybe the most common target of the attacks), the physical interfaces that provide access to the device (serial, parallel, and infrared/optical ports), the electronic components that store data (EEPROM, Flash, RAM), the buses that pass data between components (parallel and serial buses), the wireless communication protocols, and the two way communication.

In the case of the first threat, the energy usage fraud, besides the existence of many frauds related to electromechanical meters currently in use in Brazil, there are also record of frauds related to others new electronic devices, for instance pay TV [5]. From this context, it is possible to infer that the new smart meter devices to be used in Brazil will further increase the current level of fraud. Hacker attacks against the new meters are likely to occur. This kind of threat also includes attacks executed only for fun, to show how easy it is to change the energy consumption data in the meters.

User privacy violation, the second threat, is another important issue when analyzing smart meters security [6]. The metering data may reveal some customer behaviors, determining when they are at home, at work, or traveling. When at home, even specific activities may be deduced. It was recently approved in Brazil a law addressing Internet Privacy and it is also being studied the Privacy issue in the Smart Grid environment as a part of another R&D project, funded by ANEEL. Thus, the metering data stored in these smart meters are also the target of attacks, being necessary, therefore, to fully test the encryption mechanism used to protect them.

Considered perhaps the most dangerous threat, the propagation of malware over the AMI, could cause irreparable loss to the entire energy sector. In this case, an analogy can be made with the spread of a computer virus over the Internet. The recent outbreak of Stuxnet worm is a real example in the nuclear facilities [7]. Indeed, the overarching goal of an attacker is to try to identify vulnerabilities that allow expanding the control of a single device to other devices with limited or no physical access. The aggravating factor related to the Brazilian context is that, in a short period of time, all old meters will be replaced, increasing the risk of adopting vulnerable smart meters if the process occurs without care.

At last, but not least, the existence in the smart meters of a functionality for remotely interrupting the energy supply can be maliciously used as part of a physical attack. Consider for instance that a thief wants to invade a store, protected by an alarm system connected to an uninterruptible power supply. In order to commit the robbery, the burglar could simply cause a power cut and wait until the batteries get drained and the protection system is disabled. A worst scenario to be considered consists of simultaneously and persistently replicating the aforementioned attack to every single building of a city or a major area, which would quickly lead to total chaos.

Although some research activities are being conducted, there are still several threats related to vulnerability exploitation in smart meters. This section addressed the four main threat cases in the Brazilian scenario. Various types of possible attacks can result in the materialization of these threats. For this reason it will be necessary to map and study them, so that tests can be performed on these devices just as they are tested in the metrological aspects (already performed in Brazil). The following section discusses some possible attacks against smart meters, related to this R&D project.

III. POSSIBLE ATTACKS

Before presenting the possible attacks against smart meters, it is important to understand their architecture and main components as illustrated in Figure 1. Generally, there are two processors: one for calculating, with the aid of the current and voltage sensors, the energy consumption, which is showed on the LCD, and the other for processing and transmitting the collected data, besides implementing additional functionalities such as access control and firmware management, for example. The smart meter firmware and configuration parameters are stored in the EEPROM and/or flash memory modules and can be remotely updated if necessary. Several modules are responsible by providing the communication layer, using technologies such as PLC, GSM/GPRS, ZigBee, and WiFi. Examples of buses used to interconnect these components include SPI, I2C, and SMbus. Maintenance can occur using the aforementioned network protocols or through an optical port compliant with the ANSI C12.18 specification.

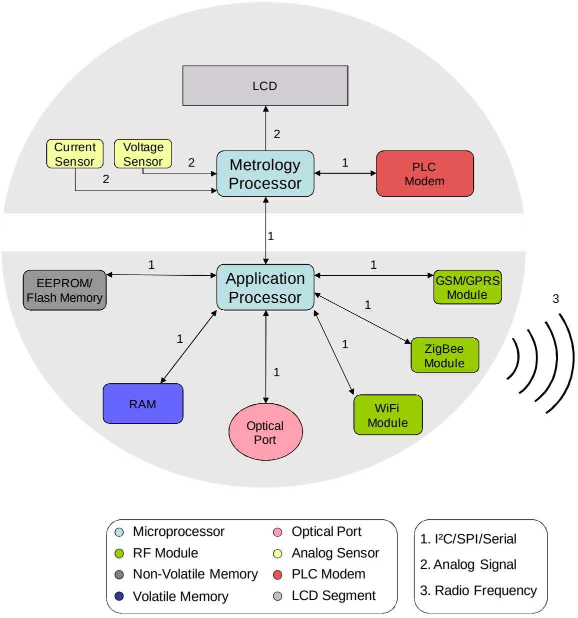

Figure 1. Smart Meter Anatomy

Recently, discussion has been growing about security attacks on smart meters. As a matter of fact, some research was done focusing on the "smart meter pentest" subject. The initial stage of this present R&D work covered the research of known attacks that are related directly to the mapped threats in the Brazilian scenario. Four works are distinguished: in [8], some general weaknesses are listed, including some hacking methods used on the devices; in [9], some interesting attacks against smart meters are explained; in [10], a methodology of attack on AMI is addressed; and in [11], a pentest model for smart grid is proposed with focus on smart meters.

Attacks on smart meters generally start by the physical interaction with the device usually performed through an optical port. In general, the first obstacle in accessing the meter is to bypass the authentication mechanism. However, some meters still do not have password or use the default manufacturer password. When using robust passwords, two possible attacks are the attempt to extract data from hardware components and the use of brute-force methods. The first one depends on the comprehension of the smart meter anatomy, as shown in Figure 1.

When accessing the device, after the successful authentication, smart meters can be connected to laptops through optical probes. This method is generally used by the company's field technicians who perform maintenance and conduct configuration changes in meters' setup. Attackers can use the same method to start their attacks. A slight change in the meters' setup data is considered an attack, as this can increase or decrease the energy consumption data. Furthermore, these changes may allow non-authorized communication with other meters, aggregators or non-AMI networks.

Another type of attack includes tampering hardware components in order to damage the device. Some smart meters contain tamper-protection mechanisms, although this type of control may fail after massive exploration. This kind of approach is initiated by gathering the available documentation such as components datasheets, operation guides and schematic diagrams. After the initial evaluation, the next important stage is to identify the weaknesses in the electronic components, for instance, the traffic of confidential data (e.g.: passwords or encryption keys) that runs between the components in a non-secure way. In this case, logical analyzers and oscilloscopes are used to help establish the type of traffic and evaluate the reading possibility. Another more advanced attack technique, related to this issue, is the use of hardware reverse-engineering techniques that makes possible the introduction of tampered components into smart meters. This type of attack is classified as hardware hacking.

Another category of attack is the attempt to access the data stored in the meter's components such as RAM, Flash memory and EEPROM chips. For the EEPROM, access is performed while the device is deactivated using the following tools: total phase beagle sniffer, bus pirate, syringe probes and JTAG programmers. Based on the dumped data, search for relevant information is performed focusing mainly on the following: (1) encryption keys and (2) firmware. Other executable codes, configuration data and files, in addition to the meter's authentication passwords or IDs, if obtained, can be useful to the attacker to run other attacks.

The attempt to find encryption keys can be performed through a simple search for basic strings (obvious keys) and entropy analysis techniques. The access to the smart meter's cryptographic keys can result, for instance, in the impersonation of the victim's smart meter, by the attacker, within the Neighborhood Area Network (NAN). Another aspect is the access to other meters that share the same symmetric key that the one which has been discovered. In any case, the impact can be enormous.

Software design flaws are the most common source of security weaknesses. Memory corruption vulnerabilities like stack overflows, heap overflows, format string, use-after-free, and off-by-one overwrite, can be exploited aiming information disclosure and arbitrary code execution. Code injection vulnerabilities like SQL and XML injection can allow improper access to user private information, device and network configuration parameters, enterprise private data, etc.

Attackers usually target firmware image recovery, as from their perspective it may drive many other attacks, like those related to software flaws. When obtaining the firmware source code, search for vulnerabilities can be performed through static analysis. When this is not possible, the alternative is to perform reverse-engineer of the firmware binary. This technique can be used to identify hard-coded strings like encryption keys and device passwords. Furthermore, firmware reverse engineering can be used with fuzzing tests [12] to identify software implementation flaws as well. The impact of attacks that explore firmware flaws goes from denial of service to total device compromise. It is important to emphasize that the binary code analysis, if demanded, is time-intensive and requires professionals with highly specialized skills.

Another attacking approach addressing the firmware consists of replacing it by a malicious version, using the remote update functionality present in most smart meters. Vulnerabilities in the way they verify the authenticity of the code to be installed could be used by such an attack. In the worst case, one can consider devices that do not authenticate the new firmware at all. A much more advanced possibility, however, involves breaking the code authentication mechanism employed by the meter. A real example of the latter, in the context of operating systems, is the technique used by the flame malware [13] to camouflage as a valid Windows software update. In this case, it was necessary to improve Stevens's cryptanalytic attack against the MD5 hash function [14], in order to make the attack possible.

IV. R&D Brazilian Project: Meters Security

This Brazilian R&D project is a 24-month program that includes the following phases: Phase (1) the state-of-the-art analysis of smart meters security: includes the research process on the already identified main vulnerabilities, attacks related to device intrusions both on the software and the hardware; Phase (2) elaboration of a methodology able to evaluate meter security and to build the Smart Meter Cyber Security Laboratory: covers the development of a methodology for testing, which will be used in the replication of future smart meter evaluations, and also includes the deployment of two laboratories, one for vulnerability research and discovery, located at CPqD, and another twin laboratory for running security tests, located at Elektro; Phase (3) execution of the hardware and software security tests in smart meters: considered the core of this project, addresses the smart meter pentests, the prospecting of new attack methods and the specification of minimum requirements for security taking into consideration the Brazilian scenario; and Phase (4) transfer of knowledge: deals with the transfer of knowledge to Elektro's team and the presentation of final results to the R&D committee and to the regulatory agency.

After the first phase of this work, it was prepared a survey addressing the main vulnerabilities and most relevant attacks on smart meter devices that were discussed during the latest security conferences worldwide. Considering the threats in the Brazilian scenario, it was possible to preliminarily ratify the elevated risk facing the replacement of all meters in Brazil. Considering the meters strength, in terms of security, which changes depending on the device, one can conclude that their conception is not based on requirements regarding information security.

Some laboratories in Brazil are already accredited by Inmetro to perform tests on meters. However, the information security tests are in initial stage in the country. The Smart Meter Cyber Security Laboratory will be the first of its kind in Brazil and will focus mainly on security tests. This laboratory can be used as the basis for the deployment of other similar laboratories elsewhere. Based on the results obtained from this R&D project, a set of minimum requirements for software integrity and security will be proposed, in addition to the procedures to check the compliance with these requirements. In the future, these items could be incorporated to the current Inmetro requirements. Currently, the project is in the phase of structuring the laboratories, acquiring equipment and testing tools.

V. Conclusions

By the beginning of 2014, power supply companies in Brazil will have to be ready to replace all their current meters. Considering the preliminary analysis, based on scientific papers and presentations that took place during the main security conferences, the replacement of meters may cause irreparable damage to the Brazilian energy sector. For this reason, research and development investments in the evaluation of software security for smart meters is crucial, mainly in the current Brazilian scenario. The results of this program will help the entire energy sector in Brazil through the creation of the first laboratory in the country, concentrating on information security tests including the specification of all features, tools and procedures to check the smart meter robustness for security baseline.

Acknowledgment

This research project has been carried out in partnership between CPqD Foundation (independent institution focused R&D and innovation) and Elektro (the eighth largest power supply organization in Brazil) and relies on R&D financial resources provided and managed by ANEEL.

References

[1] S. Fries, "Securing the Smart Grid", The First International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies - ENERGY 2011, Keynote Speaker, Presentation, May 2011.

[2] Technical briefing: “Attacking the Smart Grid,” Insights on governance, risk, and compliance - Ernst & Young, December 2011.

[3] H. Khurana, "Smart-Grid Security Issues", Security & Privacy, IEEE, Volume: 8 , Issue: 1, pp. 81-85, February 2010.

[4] W. Sikora, M. Carpenter, and J. Wright, "Smart Grid and AMI Security Concerns", InGuardians & Industrial Defender, Presentation, July 2009.

[5] Art Presse, Pirataria em TV por assinatura chega a 11,44 milhões de lares na América Latina, October 2012.

[6] B. Murrill, E. Liu, and R. Thompson II, "Smart Meter Data: Privacy and Cybersecurity", Congressional Research Service, February 2012.

[7] N. Falliere, L. Murchu, and E. Chien, "W32.Stuxnet Dossier", Symantec Security Response, Version 1.4, February 2011.

[8] M. Davis (IOActive), "SmartGrid Device Security: Adventures in a new medium", Black Hat USA, July 2009.

[9] D. Weber (InGuardians), "Looking into the eye of the meter", DEFCON 2012, July 2012.

[10] InGuardians, Inc., "Advanced Metering Infrastructure Attack Methodology", March 2011.

[11] J. Searle (UtiliSec), "Dissecting Smart Meters", Black Hat Europe 2012, March 2012.

[12] American National Standard Protocol Specification for ANSI Type 2 Optical Port, ANSI C12.18-1996, April 1996.

[13] sKyWIper Analysis Team, “sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks”, May 2012.

[14] M. Stevens, A. Sotirov, J. Appelbaum, A. Lenstra, D. Molnar, D. A. Osvik, and B. de Weger, “Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate”, in CRYPTO 2009, Lecture Notes in Computer Science, vol. 5677, pp. 55-69, August 2009.