A Smart Metering Scenario

Jorge Cuellar (Siemens AG),
Santiago Suppan (University of Regensburg and Siemens AG)

May 10, 2013

Abstract

By 2050, up to 70% of the urban population will be living in cities worldwide. This progress aggravates many challenges such as an appropriate electrical power supply. The current energy supply is an out-of-date infrastructure, which is afflicted by many problems, such as high costs, blackouts and overloads. The energy supply problem has been tackled by a number of different initiatives and funded research projects, which have established the Smart Grid as the proper solution. While security and privacy research advances rapidly, holistic and clear descriptions of privacy and security measures for the industry have been missed or postponed for future standardization.
This short scenario paper encourages future information security practitioners, particularly students or young professionals, to concretize their results by applying them to the clearness provided in this simple scenario.

Chapter 1 introduces a common terminology for the scenario description. Chapter 2 describes the scenario environment, which details the communicating parties and the exchanged information. Chapter 3 illustrates some possible worst cases in more specific situations, considering too particular attackers and threats, which can be derived from the root scenario in Chapter 2. These worst cases should help researchers to concretize their research objectives in a clear and simple way.

1 General Context: Smart Grid Security

The Smart Grid is a large, flexible, self-monitoring, auto-balancing, and self-regulating infrastructure which uses ICT to gather and respond on information in an automated manner in order to improve the efficiency, reliability, and sustainability of the production and distribution of energy.

The core of a Smart Grid depends on intelligent, reliable, secure and cost effective technology. The Smart Grid can be characterized as a combination of two infrastructures, the electrical grid carrying the energy and maintaining the safety, availability, and performance of the grid, and the information infrastructure used to supervise and control the electrical grid operation, see [1, pg. 2].

Controlling and continuously stabilizing a large grid of many dynamic components while reacting to real-time conditions and demands, is a major challenge that has to be tackled by the electrical grid automation. If this goal can be accomplished, then load peaks can be avoided and the electrical infrastructure can be reduced in size, creating great cost reductions.

To enable a dynamic load control, fine-grained and flexible automatic reports of consumption and production are required. This is provided by the combination of Smart Meters and Home Gateways with the electrical grid automation. Their main value is to save energy and costs in interplay with market mechanisms like commodity brokerage, see [2, pg. 2].

Fine-grained data documenting the production and consumption of electricity by end users can reveal a lot of personal information. The relevance of information security and privacy protection for Smart Grid infrastructure has been increasingly acknowledged over the last couple of years. The Smart Grid in general is addressed by a number of different initiatives and funded research projects investigating scenarios and use cases. Several of them address security issues specifically, like the interagency report from the National Institute of Standards and Technology (NIST IR 7628), the European Smart Grid Coordination Group (SG-CG), or by funded projects like FINSENY (Future Internet for Smart Energy), see [3, pg. 3].

The following market roles are found in a typical Smart Grid scenario, but this is a gross simplification of reality. Different countries and concrete scenarios may define a variety of other particular roles, see [1, 3].

The Prosumer (consumer/producer) is typically the end customer either consuming energy and also producing energy, e.g., by using photovoltaic or wind energy as decentralized energy resources. He is also able to store energy, for instance in the batteries of the electric vehicle and to resell the energy later when the prices are higher.

Energy Service Companies (or Energy Suppliers) are responsible for the interaction with the Prosumer, performing contractual work, but the operation of the smart metering devices at the customer's premises is usually outsourced to so-called Meter Point Operators.

For simplicity, we will assume the following list of key components. Five of them (Smart Meter, Energy Management System, Smart Appliance, Home

Area Network, Home Gateway) are inside the *Home Domain*, other three (Data Communication Network, Network Gateway, Energy Supplier Server) are in the domain of the Energy Supplier. The other two (REMS, EG) are in separate domains.

SM Smart Meter. SMs are devices that record the energy consumption of appliances within a home environment and communicate this information to Energy Suppliers via a Data Communication Network, DCN. For more details, see below.

EMS The (Home) Energy Management System. We assume that the EMS is one dedicated computer, more precisely, we assume it is a web server, that allows the user to observe how much his single appliances or rooms are consuming, and also his production and storage. Here, he is also able to define his policies, describing in some detail when to buy, sell, store, or consume energy. It also hosts data management applications and directly or indirectly (via the Smart Meter) controls the Smart Appliances, see [4]. For simplicity, we assume it communicates with all other elements in the house via a wireless Home Area Network (HAN). We also assume that it is connected to the Internet, via the HG. The user is able to log on into a personal device (PC, Tablet, etc) and access the functionality of the EMS.

REMS Remote device for Home Energy Management. The user can remotely access, via some mobile applications, his EMS, access his data, or is able to modify his polices.

SA Smart Domestic Appliance. SAs are appliances that can be remotely monitored and controlled; as such, they natively include appropriate monitoring modules. For our purposes, we treat thermostats, energy generation devices (like solar panels) or charging stations as SAs: they receive Control Messages (say, commands) and send Status Information.

HAN The wireless Home Area Network, used by the Smart Meter and by smart devices to communicate with the EMS and by the EMS to communicate with the Home Gateway (HG).

HG Home Gateway or Home Energy Services Interface. HGs are devices that can access the Internet, and also via the Home Area Network, the Smart Appliances, electric switches, and the Smart Meter.

ESS The Energy Supplier Server collects aggregated billing data from the Smart Meters, plus other data from the home gateway for added value services. The ESS (or another server of the same domain) also stores the information (ABD).

MPO The Meter Point Operator is a particular role, outsourced and controlled by the Energy Supplier, with the purpose to install and maintain the main devices of the *Advanced Metering Infrastructure*, namely the Smart Meter and the EMS.

DCN The Data Communication Network, outside the premises of the end users (the Prosumers). In particular, the network enables a two-way communication between the Smart Meters, on the Prosumer side, and the Network Gateways (NG) of the Energy Suppliers. A Data Communication Network is typically implemented using a public IP network.

NG Network Gateway. The NG interconnects Home Gateways within a specific area to other Smart Grid components, such as Energy Suppliers or Transmission System Operators.

EG The Energy Generators typically operate conventional or regenerative power plants (fossil, nuclear, solar power, etc.). For us, their importance is that they receive aggregated data from the households, that is: how much energy was consumed or produced in a city area (say, at least 30 households) in a regular amount of time, say each 5 minutes.

2 Description of the Scenario Environment

This scenario is focused on the prototypical model of a private household with an Advanced Metering Infrastructure. The household is able to produce, store, and consume energy, and to regulate the corresponding amount of energy that is taken from the grid or fed into the grid depending on market prices, to communicate data for the energy network and other services, to use Smart Appliances which accommodate the household's behavior by reacting to personal preferences, and to use the electrical vehicle charging infrastructure, which supports the stabilization of the Smart Grid by providing an Energy Storage to the grid.

Fig. 1 depicts the scenario environment. The activity steps in the scenario are as follows. All communication may be assumed to be sent encrypted, but for some connections the costs of providing the necessary infrastructure (software, hardware, keys, management functionalities, etc) may be too high. The keys in the SMs and in the HGs may be assumed to be placed by the Meter Point Operator, and the keys of the HAN to be managed by the customer (end user), but other choices could be better suited. In general, an interesting, but difficult question is the key management issue, see section 3.

Raw BD Raw Billing Data. The raw data related to energy consumption, storage and production is gathered by the SM. How exactly this happens is irrelevant for our purposes. This part of the flow is out of our scope. We may assume no problems here.

BD Then, the SM processes and stores data. It communicates the data to the EMS (via the HAN), so that the energy consumption, storage, and production can be analyzed and adjusted by the Prosumer inside the household. The data is also stored by the (local) EMS.

ABD The SM sends, on the other hand, aggregated billing data (ABD) to the NG over the public Data Communication Network, which forwards it to

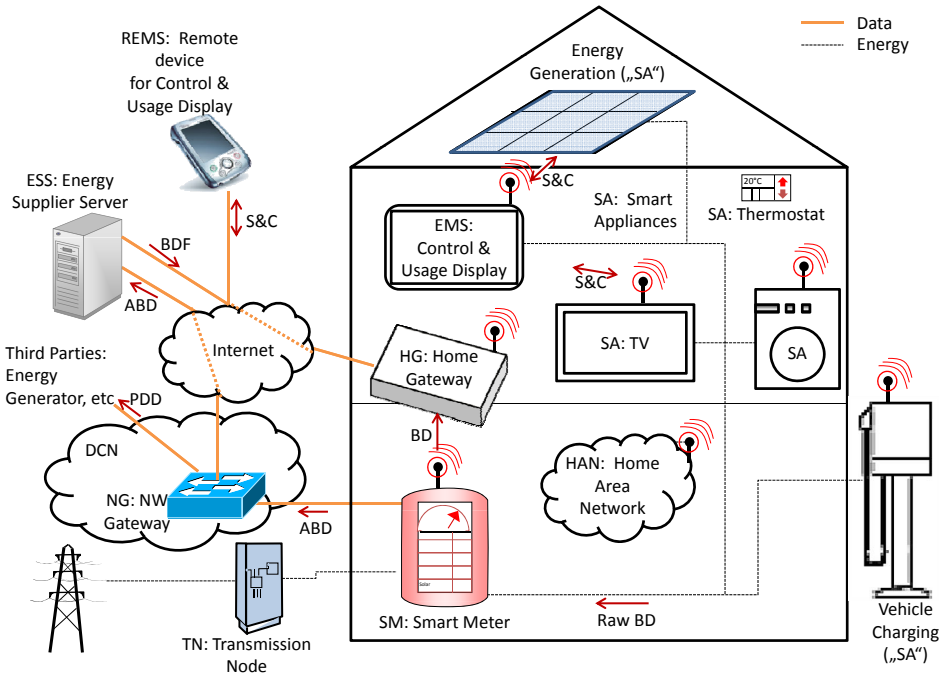

Figure 1: Case Overview: Entities and Steps

the Energy Supplier. In some scenarios, like on-demand reading, BD could be collected at low frequencies (daily/weekly/monthly), but since power metrics are required to provide real time incentives for energy savings during consumption peaks, BD are sent at high frequencies, depending on the price calculation. ABD is to be considered as personally identifiable information: it can easily be linked to the users in the household.

PDD Energy Suppliers and Energy Generators use data for power generation and distribution purposes (PDD) to obtain usage forecasts for certain sectors. PDD is aggregated BD from several households. As opposed to ABD, PDD should contain personal information only up to the point of aggregation, even if the collection frequency is high. Obviously, a sufficiently large aggregation set of different households and a trustworthy aggregation party is required. The granularity of the sectors may be fine (town area). Thereby, future energy generation can be calculated and regularized.

BDF Billing Data Feedback Information. We may assume that every five min-

utes the users are informed about their energy usage or generation volume, costs, revenues, and current rates. In this way, the EMS calculates the price of the energy that it needs for his workload, based on public energy rates.

S&C Status and Control Messages. The user locally logs on into his EMS, views the status of his devices and sends commands to the Smart Appliances or modifies the Energy Management policies. For instance, the customer triggers the activation of the washing machine. The history of actions is also stored by the (local) EMS in a log. Also, the SAs send status messages to the EMS. Status and Control Messages are also sent and received when the user is not logged in, due to rules of policies, timeouts, etc. For instance the EMS reacts to requests of appliances, or activates an SA only if enough power is available by the solar panel or public energy supply rates are low.

RS&C The user remotely logs on into his EMS via the Internet, using a REMS, say, a cellular phone or a remote PC which can be in an internet cafe. This offers him access to (a large part) of the functionality of the native EMS. The history of actions is stored by the EMS (at home, not remotely) in a log.

Inside a household a variety of persons live, whose routines differ from the ones of people in other households. Energy consumption patterns are closely tied to a persons' habits and preferences, as the Smart Appliances adapt the energy levels accordingly. Free time activities such as watching TV, but also charging the battery from an electrical vehicle can change the consumption volume significantly.

Metering and Energy Generation devices (like solar panels) are installed by the Meter Point Operator and calibrated yearly. Once installed, devices are left unattended at the disposal of the customer, unless exceptional behavior is detected.

In a particular variant of the scenario two households are at the same building, and the Smart Meters are placed in a common room, say in the basement.

3 Suggestions for Worst Cases, Attackers and Threats

The following questions should help you to analyze the scenario and more precisely, to identify the main security requirements, the possible threats (not only by external attackers but also by insiders or normal participants of the system), unwanted situations (we call them "worst cases", although they can be merely "unwanted"), and possible requirements for security in depth.

Question 1: Imagine a household inhabited by a family with children inside the premises described in Chapter 2. For an attacker, how easy can it be to know which

and how many persons are in the house? What smart-metering related data would he need? How can an attacker trace individual persons inside by exploiting the Smart Meter Infrastructure? What type of attacker can do this? Could he use this information to plan or schedule a burglary?
How could such an attack be possible?
Is the household or are even the children endangered by the misuse of, say, the Billing Data?

Question 2: As today, we should assume that different households have appliances of different types, providing different functionality. In one household, the Smart Meter, Smart Appliances and/or the House Energy Management System monitor or control the entrance door locks or the windows, the oven, the microwave, electric appliances, etc. Further, the same household may have a smart Android TV, which is a full-fledged computer, with all possible common vulnerabilities. Appliances are connected to the Internet (via the Gateway) and may receive software & key updates, system control messages and send status reports.
Do Smart Appliances introduce new threats to the Smart Metering Infrastructure?
If so, which attacker models and threats are identifiable in this scenario? Which security and privacy requirements have to be set?

Question 3: The scenario initially assumes that all the communication is encrypted. But even if this is true, is the encryption of all communication enough to guarantee privacy requirements against insider and outsider threats?

Question 4: Are impersonation attacks viable in the Smart Metering Infrastructure? Could in some cases a customer impersonate another customer? Could an attacker impersonate a server? What could happen? In which cases might this become critical?

Question 5: The scenario assumes that every communication is encrypted. How should the communication encryption be managed? Who chooses the keys, when, and how are the keys communicated to the relevant parties? At least one implementation choice may be relevant: should the system use shared symmetric keys or asymmetric ones? (Other choices could be: should the encryption be at the lower layers (network or transport layer) or at the application layer?) How should they keys be secured inside the devices? (And secured against whom?) Consider all parties involved and their possibilities to malfunction (un-)intentionally.
In your solution you may also want to consider flexibility and cost effectiveness issues, such that it can be realized in the large scale of the Smart Metering Infrastructure.

Question 6: Electric mobility and the vehicle charging infrastructure will be an integral part of the future Smart Grid. Imagine, that vehicle charging stations and vehicles exchange unique vehicle IDs (uvID). Which security and privacy

breaches could result form this approach? Which requirements should be set to avoid breaches?

References

[1] M. Rizwan Asghar and D. Miorandi. *A Holistic View of Security and Privacy Issues in Smart Grids*. Springer Lecture Notes in Computer Science, Berlin, 2012.

[2] D. von Oheimb. *IT Security architecture approaches for Smart Metering and Smart Grid*. Springer Lecture Notes in Computer Science, Berlin, 2012.

[3] R. Falk S. Fries and Ariane Sutor. *Smart Grid Information Exchange Securing the Smart Grid from the Ground*. Springer Lecture Notes in Computer Science, Berlin, 2012.

[4] Network of Excellence (NESoS). *Deliverable D11.2, Selection and Documentation of the Two Major Application Case Studies*. Springer Lecture Notes in Computer Science, Berlin, 2012.