High Assurance Smart Metering

DOI:
10.1109/HASE.2016.41

Document Version
Accepted author manuscript

High Assurance Smart Metering

Sara Cleemput, Mustafa A. Mustafa and Bart Preneel
KU Leuven and iMinds
Dept. Electrical Engineering-ESAT/COSIC
Kasteelpark Arenberg 10 Bus 2452, B-3001 Leuven, Belgium
Email: firstname.lastname@esat.kuleuven.be

***Abstract*—This paper describes a high assurance architecture for smart metering. Hacking the smart metering infrastructure can have an enormous physical impact, therefore, it is essential that the components in this architecture are proven to be secure. In order for components to be verifiable, however, they need to be sufficiently simple. In this paper, we map the functionalities and different software modules of a smart meter to a minimal number of physical components in order to obtain a cost-effective and secure smart meter. The resulting smart meter contains seven physical components: a clock, a metrology component, a display, an off-switch, memory and two processors. It contains six main software modules: a communications module, a computations module, a credit balance module and three separate security modules, one of which is implemented on the second processor. Finally, there are six strongly separated memory segments: three for log files, one for the tariffs, one for the credit balance and one containing the operational parameters.**

I. Introduction

Smart meters are globally rolled out to modernize the electricity grid. Despite the obvious importance of security in such a cyberphysical system, many of the architectures deployed today are not sufficiently secured. One potential solution, isolating the critical applications from each other and less critical applications on separate physical processors would be very expensive. Therefore, we propose a high assurance smart metering architecture using a Separation Kernel (SK), thereby obtaining an adequate level of security in a cost-effective manner. The contributions of this paper are threefold:

- It presents an analysis of a smart meter architecture.
- Based on this analysis, we perform a threat analysis.
- We propose a novel high assurance smart meter architecture based on a SK, focused on minimizing the number and complexity of security-critical modules.

A. High Assurance Systems

In high assurance systems the security and safety requirements are so critical that these systems require formal evidence of these requirements being met. High assurance system architectures are hierarchical architectures where each layer provides security mechanisms that can be used by the layer above. On top of this layered architecture of security mechanisms, a mix of trusted and untrusted applications can run isolated from each other on a shared computational system.

The lowest layer of the architecture is the SK, which provides data separation, information flow control, sanitization and damage limitation. These security mechanisms require certain hardware support; however, most commercial microprocessors and motherboards already provide the necessary features. In this paper, we will assume that the SK is commercially available. We will focus on the top layer, the application layer, analyzing the different components and modules and the information flow policy that should be enforced to ensure a secure and privacy-friendly smart meter.

B. Smart Metering

The main difference between a smart and a traditional electricity meter is the capacity for bidirectional communication of the former. The smart meter can send consumption data to the utility multiple times per hour without any manual intervention, and the utility can send commands to the meter. Smart metering fits into the larger concept of the smart electricity grid, which uses automated control to stabilize the electricity grid and increase its efficiency, thereby avoiding investments in infrastructure.

C. Use Cases

One of the main functions of the smart meter remains taking care of the **billing** process. Whereas the traditional meters are read out manually once a year, the smart electricity meter can send consumption data to the central system on a sub-hour basis and can receive commands. This capability allows adding extra functionalities to the billing process, e.g., fraud detection or efficiently switching to prepaid mode.

An additional distinct characteristic of the smart meter is the existence of an **off-switch** that can be used to disconnect the consumer from the electricity grid. This can happen for two reasons: the consumer did not pay his electricity bill, or the DSO wants to prevent a massive black-out.

One of the main motivations for deploying smart meters is the possibility to do **load balancing**. In the traditional electricity grid, load balancing is done by adjusting the supply of electricity, whereas the demand is considered difficult to control. However, with the smart meter, influencing the demand is easier, thus the consumption can also follow the production. This means the consumer can have an agreement with his energy supplier, allowing the latter to directly switch off some of the consumer's appliances, for example, his air conditioning or water boiler.

The final use case aims for energy savings by means of **consumer feedback**, i.e., giving the consumer access to detailed information about their consumption.

II. Components and applications

In this section we list the components present in the smart metering architecture and their different communication interfaces. Then, we define the applications required for each of the use cases mentioned above.

A. Components and Interfaces

The main component in the smart metering set-up is naturally the smart meter. The other components present in the architecture are: local generation, such as solar panels; other-utility meters, e.g., gas meters; the Home Area Network (HAN) gateway, also called the consumer gateway; the local maintenance technician; the top-up gateway for prepaid metering; the data concentrator; and the central system, which is responsible for all communication with the smart meter.

The smart meter consist of several components and modules. Physically separate components are: the clock, the metrology component, the display, the off-switch, the memory and the processor. The memory contains at least the logs and the tariffs. The different software modules on the processor are at least: a communications module, a computations module and a security module.

The smart meter also has six logical communication interfaces. The different interfaces are: the interface to the other-utility meter, to the HAN gateway, to the local generation unit, for credit top-up, for communication with the data concentrator and for communication with the local maintenance technician. The interface to the data concentrator is the main interface for smart meter communication, all communication to the central system also passes through this interface.

B. Applications

For each of the use cases mentioned in Section I-C, we now define the applications of which they consist.

1) Smart Billing: The core application of the billing process remains sending consumption data to the central system. Four other important applications are related to prepaid billing: switching to and from prepaid mode, billing in prepaid mode, updating the tariffs, and topping-up credit. To ensure the auditability of the billing process, logging of metrological data is critical. For all the applications mentioned so far, the data concentrator merely acts as a gateway, or has no function at all. The last application, fraud detection, is one where the data concentrator does play an important role.

2) Off-switch: There are two main cases in which the off-switch will be triggered, thereby disconnecting the consumer from the power grid. The first is when a meter in prepaid mode has exhausted its credit. The second is when the DSO wants to avoid a massive black-out and preventively disconnects some consumers from the grid. The former is an internal, or local switch-off, whereas the latter is a remote switch-off.

This off-switching is a reversible process, thus the other two applications in this use case are switching back on, i.e., reconnecting the household to the power grid, either locally or remotely. However, in the case of a remote switch-on, there should be a local confirmation that the household may reconnect to the power grid in order to avoid accidents, for example, when consumers are doing repairs on their electrical installations during a switch-off.

3) Load Balancing: The main application in this use case is switching on or off the consumer's appliances.

4) Consumer Feedback: The main application in this use case is sending consumption data to the HAN gateway. From there it can be sent on to, for example, a wall-display or the smart phone of the consumer. The second application is sending the tariffs to the HAN gateway. A third application, which is only relevant in case the meter is in prepaid mode, is sending the credit balance to the HAN gateway.

III. Threat Analysis

Starting from the use cases, we will now analyse possible threats to the smart metering architecture.

A. Smart Billing

The main threat for this use case is fraud. The main adversary motivated to carry out this type of attack is the consumer, who has physical access to the smart meter. Although the consumer's technical knowledge and resources are limited, organized crime might develop a hack and sell it to many consumers.

A second threat is the risk of privacy infringements. Both the consumption data [1], [2] and the commands potentially disclose sensitive information. The adversary, in this case, is likely to be in direct relation with the consumer, for example, an employer. However, again it seems probable that organized crime could develop the methods. Organized crime could have a second motivation to try to discover the consumption data, since these data can efficiently point them to houses with absent inhabitants, and thus, "good" targets for theft.

Although these are threats to the metering architecture, they are not the most critical threats, since an adversary cannot impact the state of the grid.

B. Off-switch

The main threat in this case would be an adversary triggering the off-switch on many different meters concurrently, causing a black-out. As soon as a large area is disconnected from the grid, this causes instability in the rest of the grid, cascading the black-out further. Beyond households, also public facilities, such as traffic lights, sewer operations, telephone networks, etc., will be affected, as all of them depend on the electricity grid. The main type of adversary who might carry out an attack of this nature would be a hostile foreign nation state or a large organized crime group. These adversaries will probably not have direct access to smart meters, but their knowledge and resources could be extensive.

A relatively low-impact threat might be an attempt to prevent a smart meter from switching off, or if already switched off, an attempt to switch it back on. Similar to billing fraud, the main person motivated to do this would be the consumer himself; however, again, consumers may obtain the hack from organized crime groups.

C. Load Balancing

Again, the main threat would be an adversary sending a command to switch off the consumer's appliances. The threat is less critical than in the case of the off-switch, since only a few of the consumer's appliances would be impacted, and only those which the consumer had already agreed to be switched off for load balancing purposes. One of the motivations of the adversary could be to harm the supplier, since consumers are likely to become annoyed and opt out of the load balancing program. A second possible threat is an attempt to break appliances by very frequently switching them on and off.

The main strategy to mitigate these threats is for the meter to perform checks to assess whether the load balancing related commands are reasonable. One could, for example, limit the number of times the appliances can be switched off in one week and require a minimal amount of time between consecutive switches in the state of appliances.

D. Consumer Feedback

Here, the main threat would be an adversary attempting to use the HAN gateway to get access to the smart meter. A second, less serious threat, could be an attempt to adjust the consumption data sent to the HAN gateway, such that the consumer does not receive the correct feedback. A privacy threat might also arise in this case, although this is much more limited than in the billing use case, since an adversary needs to be in the vicinity of the consumer's premises in order to intercept the data.

E. General Threats

An additional, very critical threat would arise if the adversary used a smart meter as an access point into the central system. Once an adversary has access to the central system, he can heavily influence the grid, for example, by sending out off-switch commands to all smart meters.

An adversary could also try to alter consumption data or commands while they reside in the data concentrator, since the data concentrator is physically accessible to a motivated attacker and contains data of many different meters.

Another general threat is that an adversary could tamper with the logs, thereby covering his tracks after executing one of the aforementioned attacks. A simple variant of this attack would be to fill up the logs with less critical events. A related threat would be if an overflow in the consumption logs overwrites data in the security logs.

IV. Proposed Architecture

We propose a cost-efficient, high-assurance architecture for the smart meter, as shown in Fig. 1. We propose adding an **additional processor** on which to build a separate security module for the off-switch, since this is the most critical component in the smart meter. Hacking this security module effectively could allow the adversary to disconnect consumers from the grid. We assume that each smart meter has off-switch keys which are independent of the off-switch keys on any other smart meter. This independence of keys allows us to avoid the use of a secure element, which would be expensive, since even if an adversary manages to carry out a side-channel attack and discover the keys, he could only obtain the keys used by one specific smart meter.

Regarding the local switch-off and switch-on commands, we propose that the credit balance module should be unable to directly communicate with the off-switch. The **only input to the off-switch should come from the off-switch security module**. Therefore, the credit balance module should send the off-switch command to the off-switch security module.

In the main processor, the following modules were already defined: the credit balance module, the communications module, the computations module and the security module. In the main memory the following segments are minimally present: the logs, the tariffs, the credit balance and the prepaid flag. We propose these different modules and memory segments be strongly isolated from each other. This requires a high-assurance system, with a lower layer, or **SK**, which must at least possess the four basic properties mentioned in the introduction: data separation, information flow control, sanitization and data separation.

Next we propose to **divide the logs** into a metrology, security and off-switch log. The metrology log will hold the consumption data together with a time stamp. The security log will hold all of the following events: commands to switch from and to prepaid billing mode, top-up attempts, commands to update the tariffs or commands to switch appliances on or off. Note that for all of the commands, an event will be logged independent of whether the command was valid. The off-switch log will hold all instances where the meter received a command to switch off or on, as well as any instance in which the off-switch was triggered due to a zero credit balance. The SK ensures that events in any of the three logs can never overflow into the other logs. An adversary would thus be unable to flush out an off-switch command he sent to the meter by sending a rapid succession of less critical commands.

Moreover, we propose to **divide the security module** into two modules, one for communication with the central system (labeled as CS security in Fig. 1), and another one for communication with the data concentrator (labled as DC security). Although the messages to and from the central system will go through the data concentrator, end-to-end encryption between the smart meter and the central system ensures a complete logical separation between these two data flows. Thus, it is logical also to separate the security mechanisms used to protect to both flows. Note that such a separation has the additional advantage that the consumption data sent to the data concentrator, which are only necessary for fraud detection, can be encrypted in such a way that the data concentrator has access only to the aggregate and not to the individual values. This can be done by using for example homomorphic encryption schemes [3].

Regarding the interface to the external components, **all communication must go through the communications module**. All incoming messages should moreover go from the communications module directly to one of the security

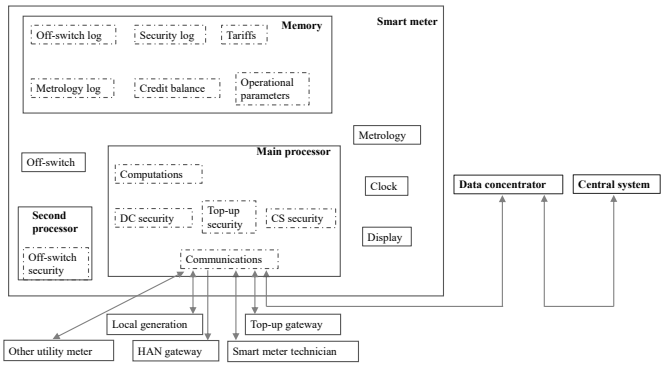

Fig. 1. Overview of the proposed archtitecture, physical components are in full lines, software modules and memory segments in dotted lines

modules, before being sent to any of the internal components or modules. This measure is required because all incoming communication is a priori untrusted, since an adversary could easily use one of these interfaces to send his own messages. Since all outgoing messages are also authenticated and (possibly) encrypted, all outgoing communication should also first pass through a security module before going to the communications module. The reason we do not combine the communications and security module into one big module is that this would make the module much more complex, violating the principle of modules which are simple enough to be formally verified.

Furthermore, we propose the **interface to the HAN gateway be a data diode**, i.e., only one-way communication is possible, from the smart meter to the HAN gateway. This is possible since in our architecture, there is no need for the HAN gateway to communicate anything back to the smart meter. One could argue that in the case of load balancing, a confirmation needs to be sent to the central system if the appliances are turned off. However, we argue that this is unnecessary, since this can simply be learned from the drop in the consumption values. Note that the main advantage is that none of the connected appliances now need to be trusted, since they cannot influence the smart meter. This greatly improves the flexibility of the in-home part of the smart metering architecture, since any new appliance can simply be added.

V. Related Work

Rushby [4] describes how partitioning can be used in the avionics sector. Two main differences with our case are that only accidental faults are considered, no adversaries, and that real time constraints are much more strict in avionics.

Anderson [5] describes some of the high-level threats to a smart grid. He identifies the main use case for smart metering as the ability to easily switch between normal billing mode and prepaid mode. He also introduces the idea of the open home controller to control the appliances of the consumer.

Sancus [6], TrustLite [7], SMART [8] and D-MILS [9] all describe possible SKs, which could serve as the lower layer for an architecture such as tours. TrustLite describes a SK for devices with very low energy resources, SMART provides a mixed kernel, containing both hardware and software elements. Sancus provides a SK for high-end embedded systems.

An accounting register dedicated only for storing meter data used for billing is introduced by Mustafa et al. [10]. To the best of our knowledge, no-one has defined all the necessary separations within a smart meter to enable formal verification.

VI. Conclusions and Future Work

Most of the existing smart metering architectures are not sufficiently secure. Those which are secure, like the German smart metering architecture for instance, are prohibitively expensive. Moreover, the German architecture is certified in the Common Criteria, and therefore, may never be changed. Thus, we have proposed a high-assurance smart meter architecture, based on a SK, which strongly isolates different software module and memory segments from each other. This architecture is updatable, since it is possible to add new modules and memory segments as needed.

Future work includes a proof-of-concept implementation of our proposed architecture to test its feasibility and provide a better estimate of the implementation cost.

Acknowledgment

The authors would like to thank B. Defend, K. Kursawe and C. Peters from the European Network for Cyber Security for their many useful suggestions and help. The research leading to these results has received funding from the European Union Seventh Framework Programme FP7/2007-2013 under grant agreement No 610535 - AMADEOS and from the Flemish Government, FWO.

References

[1] M. A. Lisovich and S. B. Wicker, "Privacy Concerns in Upcoming Residential and Commercial Demand-Response Systems," in *Power Systems Conference*. Clemson University, 2008.

[2] G. W. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870–1891, 1992.

[3] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in *Advances in Cryptology - EUROCRYPT '99*, ser. Lecture Notes on Computer Science, 1999, vol. 1592, pp. 223–238.

[4] J. Rushby, "Partitioning for avionics architectures: Requirements, mechanisms, and assurance," NASA Contractor Report CR-1999-209347, 1999.

[5] R. Anderson, "Smart meter security: a survey." [Online]. Available: https://www.cl.cam.ac.uk/ rja14/Papers/JSAC-draft.pdfs

[6] J. Noorman, P. Agten, W. Daniels, R. Strackx, A. Van Herrewege, C. Huygens, B. Preneel, I. Verbauwhede, and F. Piessens, "Sancus: Low-cost trustworthy extensible networked devices with a zero-software trusted computing base," in *22nd USENIX Security Symposium*, 2013, pp. 479–498.

[7] P. Koeberl, S. Schulz, A.-R. Sadeghi, and V. Varadharajan, "TrustLite: A security architecture for tiny embedded devices," in *Proceedings of the Ninth European Conference on Computer Systems*, ser. EuroSys '14. ACM, 2014, pp. 10:1–10:14.

[8] K. E. Defrawy, A. Francillon, D. Perito, and G. Tsudik, "SMART: Secure and minimal architecture for (establishing a dynamic) root of trust," ser. NDSS Symposium, 2012.

[9] D. Bytschkow, J. Quilbeuf, G. Igna, and H. Ruess, "Distributed MILS architectural approach for secure smart grids," in *Smart Grid Security*, ser. LNCS, 2014, vol. 8448, pp. 16–29.

[10] M. A. Mustafa, N. Zhang, G. Kalogridis, and Z. Fan, "MUSP: Multi-service, User Self-controllable and Privacy-preserving system for smart metering," in *IEEE ICC*, 2015, pp. 788–794.