Security and Privacy in Smart Grid Infrastructures

Alessandro Barenghi
Dipartimento di Elettronica e Informazione
Politecnico di Milano, I-20133 Milano, Italy
barenghi@elet.polimi.it

Gerardo Pelosi
Dipartimento di Elettronica e Informazione
Politecnico di Milano, I-20133 Milano, Italy
pelosi@elet.polimi.it

Abstract

Adding digital intelligence and two-way functionalities to the power grid is one of the most flourishing topics in both academic and public institution communities.
Efficiency, improved reliability and safety are the benefits promised by the new smart grid at the price of privacy and security challenges which are only in part similar to the security issues of IT networks. We survey the current grid architecture and the relation among the smart grid operators to analyze the security and privacy threats which needs to be addressed to secure the smart grid digital infrastructure.

1 Introduction

A key requirement for technological advancement is represented by a precise and efficient management of the energetic resources of the planet. In particular, smart management of the whole production, transmission and distribution chain of electrical power supply has become become a subject of prime interest for both academic and industrial communities. A set of technologies, commonly regrouped under the names of *smart metering* [4] and *smart power grid* has been proposed to raise the production, transmission and distribution efficiency of the present power grid infrastructures through accommodating a two-way flow of electricity and metering data.

A smart grid promises reduced vulnerability to unexpected hazards, lower energy prices, increased use of renewable resources, and fewer energy shortages [5]. The technological challenges encompass problems ranging from the integration of high-speed, low-latency telecommunications infrastructures (that can process large-scale data securely across a multiple network components) to the processing of large volumes of data received in near real-time from a multitude of remote sensors and field devices. In this sense, the ICT structure of the new smart grid will converge to a full fledged informative system, effectively speeding up the processing of the metering information on a large scale. However, the major concerns about smart grids are posed by the potential security problems raising from the network transmission of end-user's metering data and from the collection of large amount of micro-data which can introduce novel threats to customer's privacy. In addition to these concerns, security issues raise from the fundamental need to prevent denial of service attacks on the power grid, as these would cripple substantially all the modern living infrastructure [15].

The paper is organized as follows: Sect. 2 provides an overview of the current power distribution architecture and the roles foreseen by the EU for the actors involved in the infrastructure. Sect. 3 delineates the functionalities required by the smart grid infrastructure. Sect. 4 describes the security and privacy challenges arising from the new environment. Finally, Sect. 5 presents our conclusions and points towards new research directions.

2 Smart Grid Architecture and Actors

The smart grid infrastructure ought to be designed taking into account the underlying power distribution grid facilities, exploiting them whenever possible to avoid the need for extra management ones to be deployed. Both US and EU standardization committees have begun to define the technological guidelines of the new infrastructure and the role of the actors which will be interacting in the system [3, 23]. We will present the role of the actors in relation with the current electric distribution infrastructure (as recommended by the EU [3]) to provide the grounds for highlighting the security and privacy concerns raised by the new infrastructure.

Figure 1 depicts a block diagram of the current power distribution grid, together with the foreseen actors directly involved in the smart metering process, and the position of the future Energy Service Providers (ESPs) in the system. At the present time, the actors roles resembles more or less

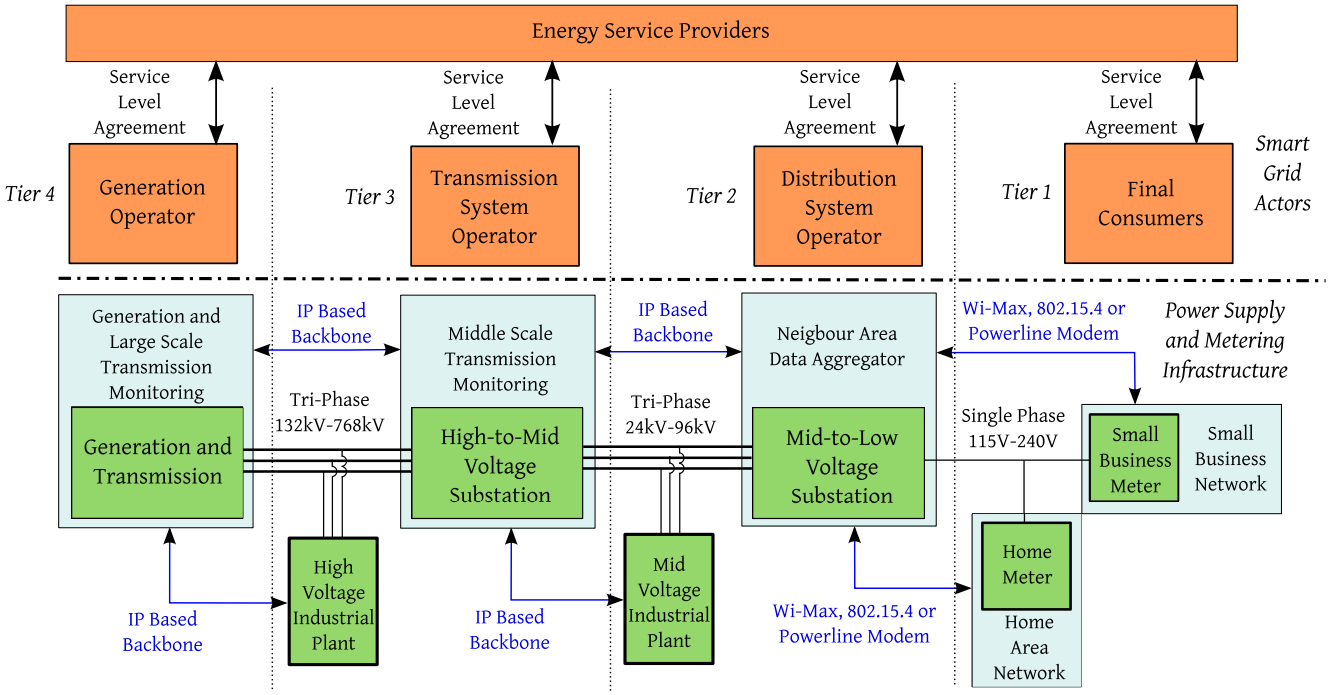

Figure 1. Power supply infrastructure and Smart Grid actors

closely the one described there, with the exception of two or more actors being actually embodied by the same physical entity, depending on the country.

In the description of the actors of the smart grid, we will follow the traditional organization of the power production and distribution grid, which comprises four tiers, according to the capacity and working voltage of the links connecting them.

The first tier is represented by the final consumers power meters and distribution lines: the power is supplied on these lines at 115V-240V depending on the country, and the loads per customer are under 6kW. The deployment of smart meters allows to monitor both the state of health of the these power lines (through collecting diagnostic information) and the typical power loads (through near real-time measurements of the power consumptions). This in turn enables the consumers, which are the actor with the key role on this tier, to have a closer interaction with the Distribution Service Operators (DSOs), which are the actor in charge of the distribution tier. In fact, smart meters are able to communicate the data they collect to the utility provider either via power line communications [20] (this strategy is mainly employed in the EU), or wireless technologies such as Wi-Max (IEEE 802.11n) [6] or ZigBee [24] (IEEE 802.15.4). This enables the DSO to collect accurate data on the state of health of the distribution lines to promptly address failures or efficiency losses in the grid, thanks to the precise location of the faulty line, thus turning the end consumers into active participants to the distribution strategies. Currently available smart power meters are also able to communicate with other utility meters such as gas and water, in order to enable remote meter reading even for utility suppliers which do not have a direct communication line with the consumer. This kind of infrastructure, denominated Home Area Network (HAN), can be exploited further to provide extra services to the customer, provided that the household appliances are able to communicate with the power meters. A common scenario is the one where the heavily demanding, non time critical appliances (f.i., e-car recharging) are automatically are scheduled for activity according to the energy plan of the consumer, achieving both savings and a reduction in power consumption spikes on the grid.

The second tier is represented by the sub-stations aggregating a hundreds to thousands of end-users, depending on the population density. These stations are usually equipped with a step-down transformer to provide to the end-user single phase low voltage (115V–240V) while tapping into the 24kV–96kV tri-phase distribution lines. These endpoints are managed by the DSO and are the prime point where it is possible to collect the measurements from the single household meters, and aggregate them obtaining local area wide power estimates. These sub-stations are usually already equipped with a common data transmission line connected to the Internet, and communicate via a Virtual Pri-

vate Network with the DSO. The monitoring actions performed on these sub-stations are primarily related to maintenance and overload prevention issues, but the foreseen evolution encompasses also the monitoring of the energy produced by small photovoltaic power plants which are owned by end consumers. As the number of these energy producers grows, the DSO will be in need to have a closer monitoring on the distribution grid, as this will act also as an entry point for generated energy. In this sense, the DSOs will be able to collaborate with the third tier and the Transmission Service Operators (TSO) through supplying them aggregate consumption and monitoring data, taking into account the productive capability of some consumers. These data can be effectively used to enhance the service quality provided by the TSO through accurate estimates of the power losses due to the aging of the grid and the identification of the zones with more demanding energy needs, which in turn need a sturdier infrastructure to be supported. The DSO will also be able to perform emergency disconnections of the meters due to safety issues (power surges on the grid) and will cooperate with the Energy Service Providers (ESPs) in order to detach from the grid delinquent consumers upon notification.

The third tier of the power grid represents the core of the energy distribution infrastructure and is based on high voltage transmission lines and high-to-mid voltage step-down stations. This tier is fully managed by the Transmission Service Operators (TSO) and provides large area energy distribution to both mid-to-low voltage sub-stations, and to a reduced number of moderately demanding industrial plants, which are directly connected to the mid voltage distribution grid and manage the step-down transformation internally. These plants usually have specific contracts with the ESP due to their high demands on the power grid, and do not have any contacts with the DSOs. These primary consumers usually have an advanced metering infrastructure already in-place due to internal maintenance issues and thus provide autonomously to solve the issues which would have pertained to their DSO and are thus able to act as a DSO for all the points pertaining to the TSO from which they are served. It is not uncommon also for these primary consumers, to have middle sized co-generation plants based on the recovery of waste heat from their productive processes, and thus them may also act as both a consumer and small energy generator[1].

The last tier encompasses the high voltage transmission power grid part connected to the power generation plants. The generation plants are attached to the high voltage transmission lines via a step-up transformation station which is managed internally by the plant. This tier is usually managed by two different actors: the owners of the power generation plants, known as the Generation Operators (GO) and the TSOs. In particular, there is a synergistic action among these two operators since, depending on the power production technology, the plants are able to supply different quantities of energy to the grid, which the TSO will be in need to distribute. Moreover, another key parameter of the power production plants is their ability to change their yield, or even turn on and off quickly according to the power demands. In particular, the power production technologies which nowadays provide the largest part of the distributed energy (coal, oil, nuclear) are not able to change their yield quickly, and cannot be turned off due to the fast equipment wear which would occur[2]. Coping with this technical issue without wasting power represents one of the key challenges of the smart grid infrastructure. In fact, since the energy consumption on the grid cannot be closely fit by a slow varying production, some mechanisms to provide extra power during peak consumption hours and to store the extra energy produced are needed. For instance, hydroelectric and geothermal power sources can be employed as large energy storages through operating the production power plant in a reverse fashion, thus acting as large power accumulators. Another solution for peak demand compensation is represented by gas power plants, which are able to perform a full start-up cycle in only fifteen minutes. Further issue in power production balancing are caused by renewable energy sources with variable yield such as solar, thermal and photo-voltaic plants or wind turbines. Since the yield of these power plants cannot be predicted accurately, the possible power outages caused by sudden yield drops represent an additional problem to be tackled by the grid wide power management. All these issues will be met by a more prompt management thanks to the fact that the TSOs of the smart grid infrastructure will be able to take decisions on the energy distribution needs based on a set grid wide, real-time measurements supplied by the DSOs, thus sensibly reducing the risks arising from a wrong consumption model of the grid. Moreover the extra power input on the grid by high yield producing regions, such as the ones characterized by a high exploitability of solar or wind resources will also be considered as effective GOs, thus raising the resiliency of the grid to partial outages due to malfunction of a GO.

On top of the actors directly interacting with the physical embodiment of the smart grid architecture, the EU reports and encourages the birth and evolution of Energy Service Providers (ESPs). The ESPs will act as energy buyers and sellers and will be interacting with the TSOs and DSOs to gain access to the power grid. The role of the ESPs will be to establish a competitive market for energy supply, taking care of buying the power produced by the GOs and delivering it to the end consumers. As the number of effective entities able to generate power will rise, the smart grid will

[1] These users are named with the portmanteau "prosumers"

[2] For instance, coal power plants burners are warranted by the constructors for only 50 power-ups

evolve to include more and more prosumers thus, the ESPs will be able to enjoy more degrees of freedom in choosing from whom to buy the required energy. The key point in the existence of the ESPs is to foster innovation and encourage an efficient management of the grid by TSOs and DSOs via a competitive behaviour, and to tackle the issue of finding the best deals for end-to-end energy providing.

3 Desired Features

After providing a description of the smart grid architecture and its actors, we will now delineate the information flows among the actors, together with the desired security properties. It is in fact a key requirement for most of the smart grid informative system to be endowed with one or more of the *confidentiality*, *integrity*, *authenticity* (as known as the CIA paradigm [1]) and *non-repudiation* properties, in order to warrant a reliable service and a clear attribution of the blame in case of violations in the service level agreements. The confidentiality property implies that only the rightful recipient of a message is able to receive it, while integrity and authenticity imply that the message has not been tampered with and has provably been produced by the rightful sender. An additional property which may be required in secure communication is the non repudiation, i.e. the sender cannot deny having sent a specific message to the receiver.

Smart Meter Communications with ESP
In the smart grid informative system, The endpoint where the information flow starts is represented by the end-consumers meters. The main advantage offered by the smart meters is the minimization of energy thefts committed by customers who manipulate the metering device. More precisely, malicious customers may either reduce the amount of measured power consumption (via voiding of the integrity of the measurements or bypassing/stopping the metre components) or offload the energy consumption of a designated final customer to another one. The extra tamper resistance of the smart meters is provided by their capability to communicate in real-time any tamper attempt to the DSO via either powerline modem or Wi-Max/ZigBee technologies. In addition to a greater resistance to tampering attacks, smart meters allow the ESPs to offer various billing plans concerning several categories of energy fares, depending not only on the quantity of the provided energy, but also on the period of the day when the consumption takes place, offering better fares during off-peak demand hours.

As it has practically proven viable to expose sensitive informations regarding a consumer via a fine grained monitoring of his power consumptions [16], the meters will need to perform the calculation of the power bill on-site and communicate with the ESP only the monthly bill. This implies that all the faring information needed to compute the power bill must be available in a timely manner to the smart meter, in order to properly compute the amount due to the ESP at the end of the billing period. The smart meters will thus need to receive the fare data from the ESP, with proper warranties of the authenticity of the data. The authenticity of the fare data is a critical aspect, both in terms of correctness of the bill computing (which could damage the end customer if it is higher than the regular due amount) or if the fare data are tampered with in order to illegally reduce the power bill. Since the meters may only physically communicate with the DSO, it is necessary to warrant the authenticity of the messages of all the messages of the ESP for which the DSO only acts as a relay and the confidentiality of the channel among the ESP and the meter.

Smart Meter Communications with DSO
In addition to the Meter-ESP information flow, the metering apparatus is in need to communicate also with the DSO, to provide useful information to the maintenance of the distribution grid. The relevant information is the fine grained measurements (every 15 minutes or less) of the power consumption of the household where the meter is installed. The DSO greatly benefits from precise and real-time measurement provided by the power meter in order to perform timely adjustments to the distribution strategies and thus prevent lapses in the service quality. These same data, after a proper area wide aggregation process, are provided to the TSO to allow grid wide load balancing and proper modeling of the global power demand. Since the DSO must not have a binding between the actual identity of the line owner and the physical line, as it would represent a clear breach of the line owner privacy [16,18,19]. It is possible to decouple them employing an anonymous ephemeral meter identifier, and tagging all the measures sent to the DSO with it (see Section 4).

The information flow sent to the DSO is characterized by confidentiality issues, as eavesdropping its contents would allow the profiling of the habits of the house served by the line by malicious entites (f.i., burglars) to determine if the house occupant is present or not. The DSO needs also to recognize the meter as belonging to the group of its own ones (although without identifying which meter it is), as otherwise a competitor DSOs could feign line faults leading to unjustified extra maintenance costs.

The descending information flow from the DSO to the meter is characterized by the need of integrity, confidentiality and authentication, since it is used to perform critical actions such as the disconnection of the meter from the power grid and the issue of software updates for the meters. In particular, the meter disconnection feature is used either in case there are safety issues, due to a grid overload, or when the ESP notifies that the line is owned by a delinquent consumer. Due to the criticality of the disconnection command, it is important that the means of issuing it impede also blind replay attacks, as even if the authenticity, integrity and con-

fidentiality of the command contents are protected, a malicious entity could simply eavesdrop a valid command an re-issue it at will.

Communications among Operators
Among the information flows characterising the smart grid infrastructure a number of them occur among the operators. The first communication among operators taking place is the one among ESP and DSO in order to issue disconnection commands. In order to prevent the disconnection of a consumer without proper reason, the communication made by the ESP to the DSO should be endowed with authentication and non repudiation properties. This provides the consumer a warranty that no-one but the ESP will be able to issue disconnection orders, and that every single disconnection order will be accounted for by the ESP. Moving up in the tiered structures, the communication taking place between the DSO and the TSO may appear as in need of only authentication and integrity, as sensitive informations about the correct working of the grid must not be forgeable, lest false ones may be injected to cause denial of service attacks [13]. However, assuming that a competitive scenario is developed among the different DSOs, confidentiality of the communication among them and the TSO becomes mandatory in order to warrant a fair market. The communication characterizing the last tier, i.e. the one intercurring among the TSO and the GOs is usually carried via ad-hoc means such as dedicated lines which are usually physically guarded over. However it is important that the physical confinement of the communication lines between TSOs and GOs is not the only method to enforce security warranties on them, since, due to the high sensitivity of the communications between large power plants and the distribution operator, the possibility of blackmails on the people enforcing the physical security layer are not negligible.

4 Security and Privacy Challenges

After delineating the information flows that characterize the smart grid environment, we will now proceed to examine the security and privacy issues on each one of them. First of all, we recall that the three cryptographic primitives able to warrant the CIA paradigm on a communication are symmetric key encryption, secure hashing and asymmetric key encryption, respectively. Symmetric key encryption protects the confidentiality of a data flow through transforming it into a non intelligible form for anyone except the possessors of a shared secret key. Secure hashing relies on computing a small digest of fixed length for a document, endowed with unforgeability properties. This implies that, given a digest it is practically infeasible to find another message with the same digest, to find two messages with the same digest or to obtain the original message back. Asymmetric key encryption provides authentication through computing a digital signature of a document with a private key so that anyone in possess of the related public key is able to verify the authenticity of the message. Since there is no computationally feasible way to derive the private key from the public one, the only possible author of the signature is the one owning the private key.

The first point to be tackled as far as security is concerned is the design of the hardware architecture and software constituting a smart meter. Usually, a smart meter is made up of a small general purpose CPU, coupled with an array of sensors, a small permanent memory to store the software and either a radio communication interface or a power line modem. The CPU elaborates the data collected by the sensors and obtains voltage, current and phase measurements from them, thus computes the amount of active and reactive power consumed [4].

The first layer of security of the meter is warranted through a tamper evident shell casing, usually endowed with specially designed seals which cannot be glued/reapplied if broken and via signalling the DSO any tamper attempt via direct communication. In addition to that, the meters are equipped with sensors monitoring the environmental magnetic field to offer a protection layer against attacks which do not involve a physical breach in the meter (as the ones reported by [13]).

Even with physical anti-tampering countermeasures in place, it is possible for an attacker to gain access to a sample meter disconnected from the network and analyze it to gain access to the software and signature keys employed to warrant the authenticity of the messages crafted by the meter. This kind of attack can be prevented through storing the keys in a battery backed up memory, and linking the blanking of the memory to the same tamper detection mechanisms employed to notify the DSO of the breach. This anti-tamper countermeasures has been recommended for its effectiveness also by NSA in order for a device to meet the highest possible security classification (Type 1) [17].

Another prime concern for the physical security of the meter is represented by the so-called *side-channel* attacks [2, 14]. This class of attacks relies on the observation of environmental parameters, such as the power consumption or the EM radiation of the implementation of a cryptographic primitive, to deduce the secret keys employed in the computations. Since these attacks can be performed with only an access to the terminals of the circuit or with a measurement of the radiated EM emissions, it is crucial that the secure chip design takes into account proper countermeasures also on this side. Employing such countermeasures prevents the falling of the secret key into malicious hands, even if the meter is analyzed separately from its working environment.

Assuming now that the content residing within the meter perimeter is safe, we move on to consider the concerns re-

garding the software running on the meter. First of all, the applications running on the device should be cryptographically signed by their owner (be it the DSO or the ESP, depending on the application). This warrants both the integrity and authenticity of the programs performing the measurements and computing the billing. It is possible to support signatures from multiple authorities through the employment of an architecture akin to the one presented for the Trusted Computing Platform [21]. This hardware-software architecture relies on a trusted boot loader, which checks as a first step that the hardware on which it is running is approved by the validation consortium through checking the off-chip component identifiers against the ones stored in the secure chip. After the hardware configuration has been validated as tamper-free, the chip checks that every program executed on the trusted platform is actually correctly signed by one of the recognized authorities, via verifying the signature on the executable binaries with one of the ESP or the DSO public keys securely stored in the chip at deployment time. A trusted computing platform is endowed with full key management capabilities and can easily handle up to tenths of warranting authorities, including the revocation of trust on compromised public keys. Through employing a trusted execution platform, the authenticity and integrity and correctness of the bill computation is warranted to the ESP, while through end-to-end encryption of the communication channel between ESP and meter it is possible to achieve the desired transaction confidentiality. To achieve non repudiation of the communications between the ESP and the meter, the device employs both the ESP public key and an ad hoc key pair generated by the ESP for the consumer, to achieve a mutually authenticated communication.

The communication with the DSO follows almost the same general guidelines of the one with the ESP. Particular care should be exercised in the fact that the DSO should send/receive messages addressed to/from an anonymous identifier of the meter. An encrypted and server-side authenticated channel must be employed to ensure the confidentiality and the integrity of the communication between meter and DSO. The server side authentication is needed in order to be sure that the meter is communicating with the actual DSO and not an eavesdropper. Particular care must be exercised in the meter disconnection messages which need to include a unique, non reusable identifier to avoid possible blind replay attacks which could be lead regardless of the fact that the whole communication is encrypted.

To assign a fully anonymous identifier to the line, no hardware parameters of the meter (such as serial numbers, part numbers, MAC addresses of the network interfaces or the unique endorsement key of the TC platform) should be employed to build the identifier. In the particularly difficult case of the Wi-Max communication [6], where the presence of a unique (meter bound) MAC address is required, it is possible to generate for each communication session an ephemeral MAC address, depending on a user specified secret and a nonce, in a non invertible way. The powerline modem does not present any implicit identification issues as the device does not have a unique MAC [20], while the ZigBee node IDs can be chosen at will [24]. The need for the DSO to identify the meters as the ones belonging to him may be solved through issuing a single secret key at customization time to all the meters. The meters will employ the secret key to compute a keyed message integrity code which enables the DSO to recognize the message as sent from a valid meter, regardless of its origin.

In addition to the in-place care about the anonymization of the measurement data sent to the DSO, it is important to consider the whole data treatment chain as sensitive under a privacy point of view. This need is mandated by the fact that it has been claimed that power consumption data may act as a valid *quasi-identifier* [12]. A quasi-identifier is a set of non-identifying attributes which are not sufficient to identify an individual when considered separately, but it becomes a valid identification metric when they are combined together (f.i., the triple gender-zip code-age in health data). Taking particular care in avoiding the leakage of quasi-identifiers is a crucial task to be undertaken to foster the diffusion of the smart grid infrastructure [11]. For instance, negligence to properly warrant the consumers' privacy has lead to a fierce opposition to the deployment of smart metering systems in the Netherlands [9].

Finally, it is advisable to have the source code of protocols and applications as publicly available to *i)* limit that exploit security vulnerabilities introduced by programming bugs [22], and *ii)* allow trusted parties to verify the correctness of the installed software [10].

5 Conclusion

This work has presented the interactions among the actors of the future smart grid infrastructure, starting from the actual power distribution architecture. After analysing which roles and which desired features are expected from an innovative and integrated power metering and distribution structure, we delineated the security issues arising from the creation of the consequent informative system. Once the main security concerns were presented, we analysed the viable solutions to the new problems outlined, through the use of available cryptographic primitives. Among the open problems, there is a growing research interest to remove either the the customization-time keying of the smart meters required to provide full anonymity in the communications between the meter and the DSO, while avoiding the introduction of a trusted third party to preserve the validation of the meters. These concerns are particularly justified in case some actors of the smart grid infrastructure are embodied by

the same entity; in particular when the ESP and DSO coincide, as they should have sensibly different behaviours with respect to the consumers' privacy. One of the most promising solutions in this direction is the use of zero-knowledge proofs [7, 16, 18, 19] based protocols, which could fit a particularly flexible market scenario, where the meters are not directly manufactured by the DSO. Another open issue is represented by the possibility to mask the power profile of a house in order to hinder the recognition of precise household appliances. One solution proposed in open literature is the one relying on the use of large batteries [8] such as the ones present in e-cars to alter the consumption profile reported by the meter, preventing the real-time identification of the appliances draining power.

Acknoledgement

This work was supported in part by the ENIAC Joint Undertaking, within the Trusted Computing for European Embedded Systems (TOISE) project, call ENIAC-2010-1, proposal number 282557-2.

References

[1] R. J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, Inc., New York, NY, USA, 1st edition, 2001.

[2] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan. The Sorcerer's Apprentice Guide to Fault Attacks. *Proc. of the IEEE*, 94(2):370–382, 2006.

[3] EU Commission Task Force for Smart Grids. Expert Group 3: Roles and Responsibilities of Actors involved in the Smart Grids Deployment, 2011, http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group3.pdf.

[4] Freescale Semiconductor. Smart Grid and Metering, 2011, www.freescale.com/files/industrial/doc/brochure/BRSMRTENERGY.pdf.

[5] IEEE. Smart Grid Conceptual Framework. IEEE Smart Grid Magazine, 2011, http://smartgrid.ieee.org/smart-grid-framework-diagram.

[6] IEEE Computer Society. IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks. IEEE Standard 802.11n-2009, New York, NY, USA, October 2009, http://standards.ieee.org/getieee802/download/802.11n-2009.pdf.

[7] M. Jawurek, M. Johns, and F. Kerschbaum. Plug-in privacy for smart metering billing. *11th Privacy Enhancing Technologies Symposium (PETS)*, 2011.

[8] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda. Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures. In *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 232–237. IEEE, 2010.

[9] E. Keemink and B. Roos. Security Analysis of Dutch Smart Metering Systems. Technical report of Universiteit Van Amsterdam, 2008, http://staff.science.uva.nl/~delaat/sne-2007-2008/p33/report.pdf.

[10] A. Kerckhoffs. La Cryptographie Militaire. *Journal des sciences militaires*, IX:5–83, 1883.

[11] R. Knyrim and G. Trieb. Smart metering under EU data protection law. *International Data Privacy Law*, 1(2):121–128, 2011, doi:10.1093/idpl/ipr004.

[12] L. Coney. Comments of the Electronic Privacy Information Center (EPIC) on Proposed Policies and Findings Pertaining to the EISA Standard Regarding Smart Grid and Customer Privacy (EPIC). Report of the Electronic Privacy Information Center (EPIC), Washington, DC, USA, 2010, http://epic.org/privacy/smartgrid/EPIC_03_10_CPUC_Comments.pdf.

[13] Y. Liu, P. Ning, and M. K. Reiter. False Data Injection Attacks against State Estimation in Electric Power Grids. In *Proceedings of the 16th ACM conference on Computer and communications security*, CCS '09, pages 21–32, New York, NY, USA, 2009. ACM.

[14] S. Mangard, E. Oswald, and T. Popp. *Power Analysis Attacks-Revealing the Secrets of Smart Cards*. Springer, 2007.

[15] P. McDaniel and S. McLaughlin. Security and Privacy Challenges in the Smart Grid. *IEEE Security and Privacy*, 7:75–77, May 2009.

[16] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin. Private memoirs of a smart meter. In *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, pages 61–66. ACM, 2010.

[17] National Security Agency. Guidelines for Type 1 Certified Cryptographic Devices, www.nsa.gov.

[18] R. Petrlic. A privacy-preserving Concept for Smart Grids. In *Sicherheit in Vernetzten Systemen: 18 DFN Workshop*, pages B1–B14. Books on Demand GmbH, 2010.

[19] A. Rial and G. Danezis. Privacy-preserving smart metering. Technical Report MSR-TR-2010-150, Microsoft Research, November 2010.

[20] STMicroelectronics. ST7538P Datasheet - Power line modem for automatic meters, 2011, http://www.st.com/stonline/books/pdf/docs/9324.pdf.

[21] J. Teo. Features and benefits of trusted computing. In *2009 Information Security Curriculum Development Conference*, InfoSecCD '09, pages 67–71, New York, NY, USA, 2009. ACM.

[22] The OWASP Foundation. The Open Web Application Security Project, 2011, https://www.owasp.org/index.php/Main_Page.

[23] The Smart Grid Interoperability Panel – Cyber Security Working Group (SGIP-CSWG). Guidelines for Smart Grid Cyber Security: Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements. National Institute of Standards and Technology Interagency Report – NISTIR 7628, Springfield, Virginia, USA, August 2010, http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf.

[24] ZigBee Alliance. Zigbee Smart Energy 2.0 Standard and Documentation, 2011, http://www.zigbee.org/Standards/Downloads.aspx#821.