Security Aspects of Advanced Metering Infrastructures

Slobodan Bojanić and Octavio Nieto-Taladriz García
Escuela Técnica Superior de Ing. de Telecomunicación
Universidad Politecnica de Madrid
Madrid, Spain
{slobodan, nieto}@die.upm.es

Srđan Đorđević
Faculty of Electronic Engineering
University of Niš
Niš, Serbia
srdjan.djordjevic@elfak.ni.ac.rs

Abstract—**The paper presents main security aspects of Advanced Metering Infrastructure in the frame of Smart Grid, where extensive use of Information and Communication Technologies makes grid smarter, but also more vulnerable to malicious cyber attacks. As a promising security solution, the Identity-Based Cryptography is particularly emphasized.**

Keywords - advanced metering infrastructure; smart grid; security; identity-based cryptography.

I. Introduction

The smart grids are upgraded electricity networks to which two-way digital communication between supplier and consumer, intelligent metering and monitoring systems have been added. Smart grids efficiently integrate the behaviour and actions of all users connected to them (generators, consumers and those that do both) to ensure an economically efficient, sustainable power system with low losses and high quality and security of supply and safety. Information and Communication Technologies (ICT) are the base platform of smart grids, that illustrates the increasing dependency of the economy and society on communication networks and computer applications. Smart grids give clear advantages and benefits to the whole society, but are complex systems where multiple actors are involved, many more than those traditionally related to power grids. The future grid thanks to ICT, will improve reliability, security, and efficiency of the electric system through information exchange, distributed generation, storage sources, and the active participation of the end consumer.

But vulnerabilities of communication networks and information systems may be exploited for financial or political motivation to shut off power to large areas or directing cyber-attacks against power generation plants. Also, software and hardware used for building the smart grid infrastructure are at risk of being tampered with even before they are linked together. Rogue code, including the so-called logic bombs which cause sudden malfunctions, can be inserted into software while it is being developed. As for hardware, remotely operated "kill switches" and hidden "backdoors" can be written into the computer chips used by the smart grid and allowing outside actors to manipulate the systems. The risk of compromise in the manufacturing process is very real and is perhaps the least understood threat. Tampering is almost impossible to detect and even harder to eradicate [1].

The smart grid will result in the deployment of a huge number of electronic and information processing devices where smart meters and the AMI communication infrastructure in general is the most significant example. Also designing and maintaining a scalable and reliable solution will be a great challenge for grid operators. Besides, this infrastructure has to be secure considering all the interconnections in place, processes (e.g. firmware updates, management actions, etc.), or even the devices themselves. Probably, system or software as a service, cloud computing, and security in depth strategies should be considered, especially in the situation of small or medium size operators.

Furthermore, physical security aspects in smart grids need special attention since the interconnection at the ICT level of households, buildings and industry with DSO and DER information networks will significantly extend the grid security perimeter. For instance, smart meters will not be under direct control of the DSO or retail providers since they will be installed inside the consumer buildings. Thus, they are at risk of being tampered (as it happened with electromechanical meters in past) and suffer a firmware hack or replacement (i.e. "flashing") so as to commit fraud or to get an entry point to the AMI network from where to craft malicious attacks or to propagate malware against other meters, smart grid applications (e.g. demand-response) or even to the back-end systems.

Many of the communication protocols currently in use for the control and automation of power generation, transmission and distribution were not designed with security in mind. Many of them were initially conceived as serial protocols with no built-in message authentication. For this reason devices will accept connections from any device trying to communicate with them mindless they are authorized or not. Besides, none of these protocols use encryption or message integrity mechanisms and as a result communications are exposed to eavesdropping and session hijacking and manipulation. Even though these vulnerabilities have been around for years, new factors have augmented the real risk [2].

On the other hand a totally new set of communication protocols is emerging so as to cope with new applications in smart grids. This is the case of AMI-related protocols such as PRIME, Meters&More, DLMS/COSEM, etc. which are being designed with security principles in mind, including cryptography for end-to-end authentication and encryption. Nevertheless, to successfully implement the highest security, cryptographic material (i.e. keys, certificates, etc.) needs to be managed efficiently and effectively which is a complex and tough task since the number of smart devices in smart grids will be really high.

The advanced metering will not only affect the power sector but also other utilities such as gas/heating and water which will make use of smart meters to remotely read and process consumption data. Synergies are possible and necessary from a business point of view. For instance, a single AMI could be used for reading any smart meter type (e.g. gas, heating, water, electricity). Data would then be delivered to the back-office systems of the AMI operator (e.g. DSO, energy retailer, gas distributor, etc). Therefore, a flexible, interoperable and well communicated infrastructure is necessary to support all information sharing needed between different utilities in an even more complex system of systems.

II. SMART GRID SECURITY CHALLENGES

Securing smart grids is a difficult task due to a series of unknown or not well understood potential vulnerabilities and weaknesses. Also, increasing the complexity of the grid could introduce vulnerabilities and increase exposure to potential attackers and unintentional errors. In addition, interconnected networks can introduce common vulnerabilities, such as communication protocol vulnerabilities or IT vulnerabilities, as well as the amount of private information exposed and increase the risk when data is aggregated. Increasing vulnerabilities to communication disruptions and the introduction of malicious software/firmware or compromised hardware could result in denial of service (DoS) or other malicious attacks. Increased number of entry points and paths are available for potential adversaries to exploit, while increased use of new technologies can introduce new vulnerabilities. Smart grids will expand the amount of collected data that can lead to the potential for compromise of data confidentiality, including the breach of customer privacy.

The key factors for the success of the smart grid are a cost reduction and fraud prevention, cyber-security of the grid, privacy of consumers and smart meter acceptance/roll-out. Thus, an end-to-end security approach at all levels of communication, from the lowest levels (meters, physical, etc.) to the upper ones (application systems, integration with corporate systems, value-added services, etc.) and all along the smart grid value chain is necessary. It includes dependencies analysis (i.e. dependencies types, business process dependencies, impact propagation, etc.) across the whole smart grid, and include security governance, use-case modeling, threat analysis, and the development of security mechanisms against distributed denial of service attacks and other attacks.

Furthermore, cyber security and privacy cannot been considered as an overlay but an integral part of the design phase to minimize costs and maximize security particularly in the near-term with the ever increasing sophistication of industrial equipment e.g. protection against zero-day vulnerabilities; optimization of very specific cryptographic protocols to reduce processing load without reducing the security level.

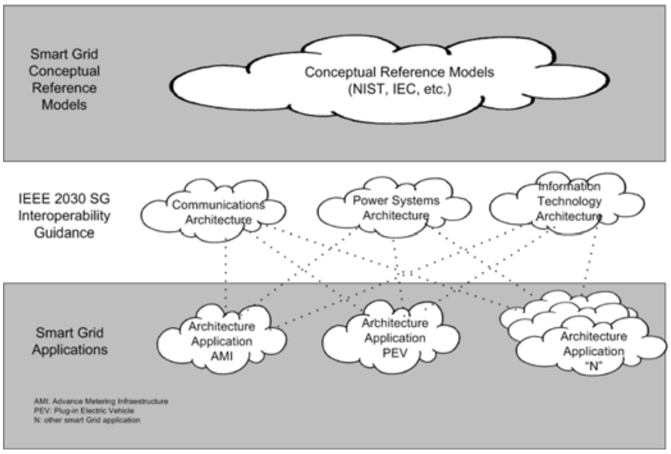
Smart Grid Conceptual Reference Models
Conceptual Reference Models (NIST, IEC, etc.)
IEEE 2030 SG Interoperability Guidance
Communications Architecture
Power Systems Architecture
Information Technology Architecture
Smart Grid Applications
Architecture Application AMI
Architecture Application PEV
Architecture Application "N"
AMI: Advance Metering Infraestructure
PEV: Plug-in Electric Vehicle
N: other smart Grid application

Figure 1. The smart grid architecture with ICT Relationship.

Also new risks for electricity delivery emerge due to the integration of the end user property (e.g. demand-response and home-based energy sources), as part of the smart grid, widely extends the attack surface area. Since it is not possible to control what is going on inside the end-customer houses it should be considered as a high-risk area, in addition to a more intensive use of the Internet and other public networks in the smart grid (e.g. DER connection, and value-added services for end customers).

New services and highly automated systems will need to monitor the smart grid more deeply by implementing new technologies. It is necessary to have a security infrastructure capable of guaranteeing trusted large scale transactions (millions of devices that could be shut down for one hour at the scale of a country, which will result in lots of payment information transactions, etc.) (Fig. 1). The architecture considerations include: self-healing and graceful degrading architectures; standard and secure interconnections among domains; management of processes associated with the use of cryptographic material (i.e. generation, distribution and storage of cryptographic material); active monitoring for attack detection and traceability.

III. SMART METERS SECURITY

Smart Meter's are envisioned to provide various functionalities in respect with the customer, grid and network support, commercial aspects of energy supply or security and privacy. Regarding the customer, they provide readings from the meter to the customer and to equipment that he may have installed; updates these readings frequently enough to allow the information to be used to achieve energy savings; provides these readings in a form easily understood by the untrained consumer, and with calculations enabling final customers to better control their energy consumption. Regarding grid and network support, a smart meter allows remote reading of meter registers by meter operators and by third parties; provides two-way communication between the meter and external networks for maintenance and control of the meter; provides for the monitoring of power quality; allows readings to be taken frequently enough to allow the information to be used for network planning. Regarding commercial aspects of energy supply, the smart meter supports advanced tariff systems and supports energy supply by pre-payment and on credit; allows remote on/off control of the supply and/or flow or power limitation. In respect with to allow distributed generation, it should provide import / export and reactive metering [4].

The smart meter's functionality regarding security and privacy is to provide secure data communications and fraud prevention and detection. This relates to both the demand and the supply side considering that privacy and security are separate and different. Privacy is the restriction of information to the customer and those authorised by the customer to have access to it, while security is the prevention of access to information by unauthorised 3rd parties. Furthermore it relates to security of communications between the smart meter and energy suppliers / grid operators, privacy of communication within a customer's premises, access to information or equipment that could lead to a breach of security or privacy; if security and privacy integral to the design of the Smart Meter System, or added.

Smart grid services and applications encompass AMI-based applications/services (e.g. demand-side management, home-energy management), distributed generation management and advanced distribution/transmission automation (e.g. substation automation, storage management, advanced distribution applications, islanding, etc.). The smart grids, and particularly the Advanced Metering Infrastructures and the introduction of smart meters in households, buildings and industry will allow DSOs to get billing readings remotely and in an automated way. Since customer acceptance is considered a key success factor for the smart grid, to that aim, privacy is considered more important than cyber security, mainly in smart meter related applications. This is the reason why privacy and cyber security are being addressed separately, although they are closely related.

The AMI infrastructure provides a two-way communication infrastructure between customers and utilities (i.e. DSOs) and it is one of the main ICT components to smarten the power grid. It heavily depends on the installation of automated meter reading (AMR) devices (smart meters) whose basic objective is measuring energy consumption, as their traditional analog counterparts. They are also able to perform operations such as measuring power usage in real-time, monitoring and informing about power quality, track customer usage parameters and keep a historical record, remotely connect and disconnect customers from the power grid, send out alarms to the DSO in case of technical issues such as component failures or loss of power notifications, react to real-time pricing signals received from the DSO or energy retailer, energy prepayment, remotely receive and install firmware upgrades so as to incorporate new functionality, anti-tampering and fraud detection, remotely customizable load limit feature.

There are other elements that are a basic part of the AMI, such as the underlying communication infrastructure, the central Meter Data Management systems or the intermediate meter data concentrators. Meter data concentrators, or just data concentrators, are Intelligent Electronic Devices that act as a gateway between MDM and smart meters. AMI together with local Energy Management Systems are key elements for achieving the objectives to not only consume power but also to produce it and having an Electric Vehicle which can be connected to the grid anywhere and anytime are related with the concepts of Smart Home/building/business/industry.

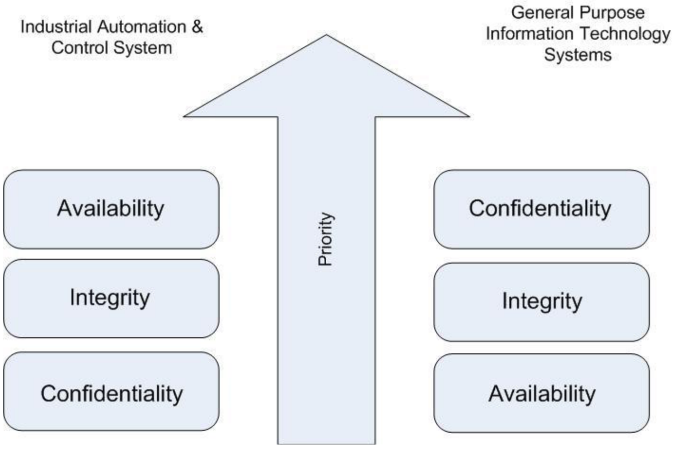

Figure 2. ICT security goals in smart grids

The smart grids' communication infrastructure spans the different domains, including transmission, distribution and even the customer premises. Security requirements for the information infrastructure of the smart grid are similar to typical corporate information systems. However, when it comes to managing the risks, strategies and priorities are significantly different and heavily depend on the domain. From an operational perspective, two major classes are grid automation and supporting ICS (e.g. SCADA, RTU, PLC, IED, etc.), and value-added service provided to end consumers and supporting infrastructures (e.g. smart meters, energy management systems, etc.) which is very much similar to traditional ICT (Fig. 2). In some cases the application will determine which security dimension is more important for a same piece of data. For instance, in demand-response applications, consumption readings coming from smart meters could be used in an aggregated manner for power flows rerouting and grid optimization. In such a case, availability and integrity is absolutely necessary to guarantee that the supervisory control system takes the appropriate decisions.

The ICT security encompasses three basic dimensions (confidentiality, integrity and availability) which define risk management priorities, classify information, characterise security requirements, etc. The authentication and non-repudiation are two other dimensions relevant for smart grid security either in grid automation or end consumer added-value energy services. In traditional IT systems information confidentiality and integrity are the main concern. For ICS systems in charge of grid automation human and equipment safety, environmental impacts and the process itself (i.e. power blackouts) are the main concerns. For this reason availability and integrity are the priorities for grid automation. On the contrary, smart metering security priorities resemble traditional ICT environment. Meter readings are starting to be considered as personal data since they provide knowledge about personal habits, thus regarding their protection and secure handling, the challenges are the possibility of inferring relevant information (e.g. particular habits) from personal data and the metering data will have to be securely accessible by several independent actors (e.g. DSO, service provider, the consumer).

IV. Identity-Based Cryptography

High levels of security are essential for all communications between the meter and the meter operator both for direct communications with the meter and for any messages that may be passing through the meter to or from any appliances or controls within the consumer's premises. For local communications within the consumer's premises, both privacy and security are required thus consumer privacy, device authentication, as well as data integrity must first be addressed before any higher-level energy policies, such as intelligent pricing strategies, can be successfully implemented.

In the smart grid, large amount of sensors and measurement devices will be used to continuously monitor the energy generation, transmission, and usage. Some data are collected every second or more frequently than other. Sensors would send their data to the smart meter installed in a household and responsible for collecting the data of all the sensors residing in that home. Traffic mainly goes from the sensors which are likely to be battery-powered and subject to energy constraint while the smart meter, does not have energy concern. Since, in smart grid, we should offload the senders of messages as much as possible, Identity-Based Cryptography (IBC) is a very promising security solution.

IBC is a public key cryptosystem introduced by Shamir in 1984 [5] while in 2001, Boneh and Franklin [6] invented the first feasible solutions for IBC using the Weil pairing on elliptic curves. Since then, many ID-based key agreement protocols and signature schemes using bilinear pairing have been suggested [7]. The main differentiating feature of an IBC is that any agree upon on and publicly available unique information about a user, such as her email address, can be used to generate the user's public key. Thus, the sender may send encrypted messages to the receiver without any prior communication with the receiver or any trusted third-party such as a certificate authority (CA). It is the responsibility of the receiver, to establish authenticated communication with a key-generating server (KGS) to obtain his private key, only if he wishes to decrypt the encrypted messages. Moreover, the receiver may keep his private key for as long as the key is valid without any further communication with the KGS. This feature greatly simplifies the cryptosystem setup and reduces key exchange data traffic,

A trustworthy CA is responsible for providing legitimate key information for all communication in many other traditional public key systems like X.509. Although public keys are not sensitive information, it is necessary to ensure that the sender acquires the real public key of the receiver, instead of fake ones provided by the intruder. Thus, before sending any message to the receiver, the sender needs to obtain a certificate from CA that contains the receiver's key. Thus in X.509, it is the sender's responsibility to talk to the KGS, while in IBC, it is the recipient's duty to obtain the key from the KGS.

IBC also allows re-keying, also called key revocation, to be initiated by the sender, which is different from conventional public-key infrastructure (PKI). When the sender wants the recipient to use new keys, he simply encrypts the packet using a new public key of her choice, such as, a key generated by using the recipient's ID appended with a timestamp. When the recipient receives packets encrypted by a new public key, he must obtain the corresponding new private key from the KGS for decryption. This allows the measurement devices to issue re-keying based on their individual needs. E.g. different devices may take measurements at different frequencies with different levels of on-board buffering. In IBC in contrast to traditional PKI, individual device can determine when to change the key according to its own data and security requirement since the same key should not be used for too many packets.

V. Conclusion

The smart grids will substantially improve control over electricity consumption and distribution to the benefit of consumers, electricity suppliers and grid operators. Thanks to ICT, the grid of the future will become smarter so as to improve the reliability, security, and efficiency of the electric system through information exchange, distributed generation, storage sources, and the active participation of the end consumer. Nevertheless, improved operations and services will come at the cost of exposing the entire electricity network to new challenges, in particular in the field of security of communication networks and information systems. AMI-based applications/services is the domain of smart grid services and applications which greatly affects the consumers' perception and acceptance of smart grid due to numerous security and privacy concerns. Identity-Based Cryptography is promising technique to secure the consumers' data and enable the adoption of smart grid.

References

[1] European Network and Information Security Agency (ENISA), "Smart Grid Security Recommendations for Europe and Member States", 01-07-2012.

[2] Commission of the European communities. "Smart Grids: from innovation to deployment". COM(2011) 202 final. 2011.

[3] National Institute of Standards and Technology (NIST). NISTIR 7628: Guidelines for Smart Grid Cyber Security. Smart Grid Interoperability Panel–Cyber Security Working Group (SGIP–CSWG). 2010.

[4] A joint contribution of DG ENER and DG INFSO towards the Digital Agenda, Action 73: Set of common functional requirements of the SMART METER , October 2011.

[5] Adi Shamir, "Identity-Based Cryptosystems and Signature Schemes" Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 7:47--53, 1984

[6] D. Boneh and M. K. Franklin "Identity-based encryption from the weil pairing," CRYPTO'01 Proceedings of the 21 st Annual International Cryptology Conference and Advances in Cryptology, London, 2001, pp. 213-229.

[7] S.H.M. Kwok, E.Y. Lam, and King-Shan Lui "Zero-configuration Identity-based Signcryption Scheme for Smart Grid," Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference, 4-6 Oct. 2010, pp. 321-326.