Smart Metering in Power Grids: Application Scenarios and Security

Alessandro Barenghi, Guido M. Bertoni, Luca Breveglieri, Maria Grazia Fugini and Gerardo Pelosi

***Abstract*--This paper gives an overview of the issues to be tackled when managing a secure smart power grid. It is targeted to applicative scenarios, namely smart metering, electric car (e-car) management and home multimedia gateway based on power-line data transmission. The ENIAC JU TOISE project concepts, wherein the paper is framed, are introduced. Then the scenarios are illustrated, the architectural model of the smart grid is described at a high level, the actors and services are identified, and the main security threats are listed.**

***Index Terms*--Power grid security, Smart Metering, E-Car, Multimedia Streaming, Trust, Security, Privacy, Tamper Resistant Systems, Physical Attacks**

I. Introduction

IN conjunction with the scientific and technologic global challenge of developing power-efficient microelectronic systems, a crucial issue is to develop energy efficient networks, designed having in mind the secure management of smart electrical grids and their related sensor networks. Consequently, methods and tools are required to develop open trusted platforms, secure storage, identification and authentication mechanisms, and tamper resistant devices, able to ensure energy management and communication at different levels of the grid, i.e. device, terminal or network. In particular, new hardware and firmware technologies are required to secure critical devices (e.g., power meters) and communications in smart power grids. This should allow bridging smart objects such as home appliances, multimedia devices or next generation vehicles, in wireless and wired networks. However, providing a secure environment, which allows to bridge these devices without incurring in problems from both malicious users seeking personal profit or external attackers willing to cause power grid disruptions presents a number of challenges. The paper is organized as follows. Section II presents the key concepts of the TOISE project, within which this paper is framed, and the applicative scenarios. Section III describes related work and emerging standards in power grids security. Section IV outlines the system architecture. Section V presents the security threats, while Section VI describes the system services in terms of modeled system functions. Section VII concludes the paper.

II. TOISE Concept

For future applications, such as Smart Grids for electricity distribution, smart- and low-energy controlled home appliances, environmental or infrastructural sensor networks, there is a need of a number of technologies to enhance the security level over communication networks, both wired and wireless, in order to yield smarter and more secure solutions, also based on trusted components. The ENIAC JU project TOISE (Trusted Computing for European Embedded Systems) [1] addresses secure and tamper resistant solutions needed by embedded applications related to power grids. Trusted Computing provides a practically validated approach to mitigate new security threats and attacks for common Personal Computers, through implementation of a chain of authentication and integrity procedures from the boot of the computing platform up to the applications set. The overall goal of TOISE is to define, develop and validate trusted hardware and firmware mechanisms applicable to lightweight embedded devices and in particular secure smart metering systems used in the smart energy grid. A second targeted application is represented by Wireless Sensor Networks (WSNs) for environmental or industrial monitoring, where security features and low-power operation, two conflicting desired features, must be achieved through reliable and sound engineering of the target platform.

The main challenges addressed in TOISE regard secure solutions required by future applications on energy grids, related to smart and networked home appliances, sensor networks and wireless communications and management of trusted objects. In fact, electrical grids require significant dependence on distributed intelligence and broadband communication capabilities. Power meters are required to control appliances at consumer homes to reduce energy. These needed capabilities require proven security technology for large, wide area communications networks. Moreover, sensor networks used for environmental monitoring, airports and critical sites safety, infrastructure monitoring, and health care are required to operate in non-controlled environments. Hence, the network can easily be compromised by an attacker. Security and survivability are crucial for applications based on WSNs. The first objective of TOISE is to investigate and implement secure solutions for the design of smart-grid applications and their deployment in large-scale networks and systems. These solutions will be based on hardware trust anchors in devices located in uncontrolled environments and will use advanced trust establishment mechanisms. The

A. Barenghi, L. Breveglieri, M. G. Fugini, and G. Pelosi are with Dipartimento di Elettronica e Informazione (DEI), Politecnico di Milano, Via G. Ponzio 34/5, I-20133, Milan, Italy (e-mail: {barenghi, brevegli, fugini, pelosi}@elet.polimi.it).

G. M. Bertoni is with STMicroeletronics, Via Olivetti 2, I-20041, Agrate Brianza (MB), Italy (e-mail: guido.bertoni@st.com).

second objective of TOISE is to investigate and implement secure WSNs to address secure authentication devices, to study and implement new generation of trusted portable devices as well secure storage in memory and study hardware secure items to add to TPM (Trusted Platform Module/TCG) for embedded system. The proposed solutions will target both lightweight low footprint secure devices and trusted anchors with complex SoC (System on a Chip) platforms. A third objective is to develop a new generation of tokens (based on several form factors) that will demonstrate to be able to provide optimal cost through full SoC integration. Moreover, capabilities such as enforced privacy management with new authentication interfaces, secure channel establishment with TPM's for secret secure updates and management of various entities will be developed. Related standardization activities are supported to promote the European solutions. As an architecture, TOISE proposes to extend hardware and firmware tamper-resistance devices architectures and/or using lightweight TPM concepts to smart grids and particularly smart-meters environments, which would address new energy efficiency in trusted applications. Also, investigating new anti-counterfeiting architectures and implementations will be provided so that they fit under the area of research on communications, wireless networks and management of trusted devices. This paper focuses on smart metering. Many concepts and technologies are akin to the ones employed in WSNs.

A. Scenarios

Smart Metering is a basic and foremost applicative scenario of the TOISE project. It consists of automatically measuring the electric power consumption of any end-consumer (e.g., a single house, an enterprise, or even a whole urban block), and of transmitting the consumption data to the utility provider, which in turn will automatically bill the consumer. It also takes care of measuring technical parameters for the provider to balance the load in the power grid, disconnect and reconnect the consumer for either contract bound reasons (i.e., unfulfilled bill payments) or technical safety reasons (such as large power surges on the grid.). Moreover, the same information can be used to manage emergencies and cope with faults, as well as generate reports and statistics. The automatic management of the utilities can be extended by metering and accounting also to other provided goods such as gas and water, through employing intelligent meters provided with a convenient data line to transmit the collected information. A second scenario regards E-Cars. It is a generalization of the final consumer smart metering scenario. It consists of having a vehicle powered by an electric engine supplied by a battery to be recharged either at home or in an equipped parking area. The E-car owner should automatically be billed for the energy employed to refill the battery pack of the vehicle. The E-car scenario has all the services of smart metering. In addition, it is characterized by services thought for parking lots and other areas, where a large number of cars are gathered and recharged (i.e., car rental stations) in order to efficiently manage their internal power reserve. A car pool can in fact act as a power consumer, on a larger scale than a home, as well as a power producer, thanks to large arrays of solar panels, although on a smaller scale than a large power plant. The third scenario considers Multimedia Streaming as another specialization of Smart Metering. It consists of locally storing and distributing copyrighted multimedia data by means of the power grid, e.g., in a house or in a building, downloading such data by means of the power grid as an alternative to using a traditional data network, e.g., the global internet. Hence also streams of applicative data, unrelated with the technical ones pertaining the smart grid architecture, could be transmitted via the same power grid means. Multimedia streaming shares all the common services of the basic smart metering, e.g., billing the consumer. However, providing the service is data intensive, because multimedia data streams may be significantly larger than technical ones, whilst being in need of fully protection against security threats.

III. Related Work And Standards

The smart grid initiatives have risen a great deal of interests, as the topic is crucial for global development. In particular, the National Institute of Standards and Technology (NIST) has developed security guidelines and a model of the power grid infrastructure for the US [2], which defines interfaces, prerequisites and implementation strategies for the smart power grid. Analogously, the Zigbee alliance [3] has now available a full-fledged wireless network solution which has been successfully deployed in the US and could be used for both infra-meter and meter-to-DSO communications. As one of its defining features, ZigBee provides facilities for carrying out secure communications, protecting establishment and transport of cryptographic keys, ciphering frames and controlling devices. It builds on the basic security framework defined in IEEE 802.15.4. This part of the architecture relies on the correct management of symmetric keys and the correct implementation of methods and security policies.The HomePlug Alliance, Wi-Fi Alliance, HomeGrid Forum and ZigBee Alliance have agreed to create a Consortium for SEP 2.0 Interoperability [4]. The consortium will enable organizations whose technologies support communications over IP. in order to harmonize the work of many industries to bring smart grid benefits to consumers. SEP 2 was selected in 2009 by the NIST as a standard profile for smart energy management in home devices. PRIME (PoweRline Intelligent Metering Evolution) is an initiative driven by Iberdrola for: “the definition and testing of a new public, open and non-proprietary communications architecture that supports remote meter processing functionalities” [5]. Its security proposal addresses security at low level, by encrypting packets. The security functionality provides privacy, authentication and data integrity to the MAC layer through a secure connection method and a key management policy. Several security profiles are provided to manage different security needs, which can arise in different network environments. Confidentiality is guaranteed by encryption and from the fact that the encryption key is kept secret. Authentication is guaranteed by the fact that each node has its own secret key known only by the node itself. Data integrity is guaranteed by the fact that the payload CRC is encrypted. Individual EU Countries have begun to standardize common guidelines for tamper proof electronic devices, able to warrant the level of physical security required by meters. For example, the German authority (Bundesamt fur Sicherheit in der Informationstechnik) has released a guideline document for tamper proof smart meters [6]. The EU has instituted a task force aimed at analyzing and building recommendations for the future of the smart grid and has released explicit guidelines regarding data protection and security in [7]. For the specific issue of privacy preserving, metering aggregation and comparison is presented in [8]. Their protocol requires a high number of bytes for interaction between the individual meters and relatively expensive cryptography on the meters. [9] highlights privacy-related threats of smart metering and proposes an architecture for secure measurements which rely on trusted components outside of the meter. [10] proposes a protocol using commitments and zero knowledge proofs to privately derive and prove the correctness of bills, but does not address aggregation across meters. Some techniques have been extended to protocols providing differential privacy guarantees [11]. In general, we in the field of smart grids, smart metering and more generally power line/ wireless communications, a large amount of standards is available, but it is not easy to understand which are relevant and where security is covered, due to the different nature of the standards and the different scope of interventions [12, 13].

IV. Architectural Reference

The TOISE project and scenarios are based on technologies which are now illustrated in their main features. A power line connection distributes electric power and data together, and uses the existing electric power grid to this purpose. It is characterized by having a reliability higher than that of the recent wireless communication technologies like the WiMAX and GPRS/UMTS protocols, as well as providing capillary access to all the households in a manner very similar to the common public switched telephone network or the local area network technologies. A group of power meters, acting as data gateways, are connected to a concentrator, which can be conveniently placed within a mid to low voltage step down substation. A low data rate and long battery life wireless connection, most likely based on ZigBee [14], can be used to provide connectivity locally among nearby meters (e.g., those displaced in a home or a building) which do not have a direct power line connection, such as the ones measuring non-electric resources like gas and water. For all such meters, the electric power meter works as a gateway to the power line connection. At an intermediate level, the concentrators are connected to both the power grid and to an IP-based network (e.g., the global internet) in order to act as a data bridge into and from power lines. The system architecture is depicted in Fig. 1. The utility companies (*Providers*) manage energy production, while *Distributors* manage the power grid and acquire metering data through the power line connections. The data concentrators are scattered along the power distributors level. Finally the "customer premises" are the level of *Consumers*, where meters of all kinds are located at individual end-customers (home or enterprise). Fig. 1 shows a generic model and of course can be simplified or refined. Meters of different types can communicate with one another via a wireless connection. The electric power meter can communicate with the concentrator via the power line connection, and eventually the concentrator can communicate with the provider via a data network. Groups of distributors and providers can work in a Virtual Organization mode, e.g., they may share customers.

A. *Actors and Services*

Smart Metering involves four different actors: provider, distributor, consumer and meter. The first three roles, shown in Fig. 1, are identified through the following labels [6]: Energy Service Provider (ESP), Distribution Service Operator (DSO), and Final Customer (FC). The ESP produces the resources to be consumed (electric power or streaming multimedia contents). The DSO, which may be the same entity as the Provider, manages (acquires and uses) metering data from the power grid. Metering data can be of two types: consumption data, namely the consumption of a resource (e.g., electric power) used for billing, and technical data, namely technical information used for power grid management. Examples of uses of technical data are: balancing the energy levels, avoiding or smoothing load peaks, disconnecting and reconnecting customers and providers. The DSO uses consumption data for payments/billing, and for formulating custom billing plans and contracts with the "fidelized" final consumer (private or enterprise). It monitors and controls the status of the access points and bridges, or concentrators, through the acquisition of technical data about the meter statuses (e.g., enabled, disabled or faulty). It also manages emergencies, generates reports on consumptions based on consumption data about consumers' groups, and, in general, it performs measurements. It controls the functionalities of the meters to check if they are operative and is also to send operational commands like "change billing contract", "connect" and "disconnect". Consumption data may also be used to generate reports and statistics, so generating profiles of consumption (e.g., for certain user classes). Since a DSO is a specialization of an ESP, it can perform also energy-related operations, possibly on a smaller scale.

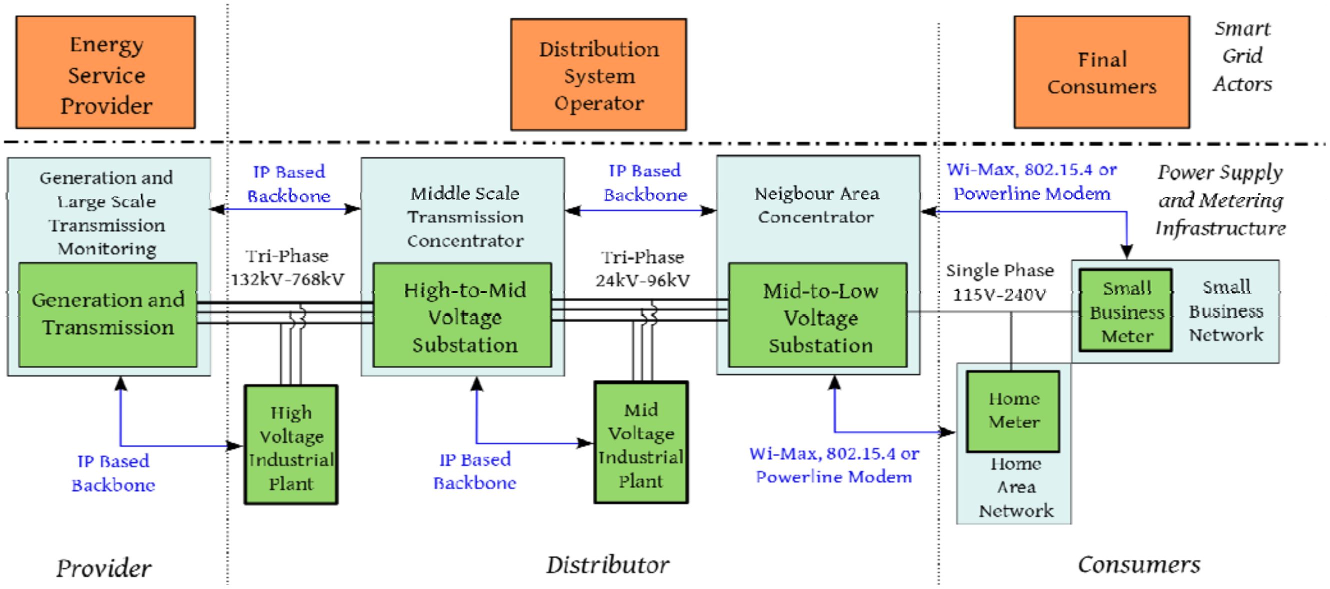
Energy Service Provider
Distribution System Operator
Final Consumers
Smart Grid Actors
Generation and Large Scale Transmission Monitoring
IP Based Backbone
Middle Scale Transmission Concentrator
IP Based Backbone
Neigbour Area Concentrator
Wi-Max, 802.15.4 or Powerline Modem
Power Supply and Metering Infrastructure
Tri-Phase 132kV-768kV
Tri-Phase 24kV-96kV
Single Phase 115V-240V
Generation and Transmission
High-to-Mid Voltage Substation
Mid-to-Low Voltage Substation
Small Business Meter
Small Business Network
High Voltage Industrial Plant
Mid Voltage Industrial Plant
Home Meter
Home Area Network
IP Based Backbone
IP Based Backbone
Wi-Max, 802.15.4 or Powerline Modem
Provider
Distributor
Consumers

Fig. 1. Layered architecture of actors components and communication in the structure of the power grid

The FC is regarded in conjunction with the meter installed at his facility. It does not directly access any kind of data. He can subscribe/unsubscribe supply contracts and require periodic reports about consumption. Indirectly he sends measurements through the meters and receives billings. The final customer consumption can also be profiled to offer him the most suitable contract. However the profiling of the customer should be done carefully as it has been proven that the profiling of consumptions of a household with a high time precision allows one to infer whether specific house appliances were active at a certain time. This information can also be exploited to infer habits of the customer, thus representing an effective breach of his privacy. For these reasons customer profiling should be limited to a time scale loose enough to prevent leakage of private information. The meter is the smart device used for the measurement of consumptions at local sites. It periodically sends consumption and technical data to the DSO. Consumption data are used for billing and technical data are used for load balancing. It can be connected or disconnected to/from the power line; it signals its operation and its faults to the DSO. It communicates over a secure channel with the DSO using symmetric cryptography, timestamps and signature, in order to authenticate the DSO and get authenticated. A refinement of smart metering is that an FC may act as a local Provider of some resource type, usually electric power, e.g., through photovoltaic power generation. In this case he will have some of the provider/distribution services, to an extent limited by the small scale of his resource generation capability.

B. *E-car scenario*

E-Car involves all the actors (provider, distributor and consumer) and has all the services of smart metering. In addition, a car concentration structure (e.g., a parking lot or a car station) may act as a consumer as well as a provider (of electric power), thus fully being a so-called pro-sumer. Therefore the e-car architecture should include services for the management of internal power reserves. The home consumer uses power to recharge one or few cars. The concentration structure basically behaves like an individual and schedules car recharging by using power from the external power grid. Additionally it can provide power: e.g., transfer power from a long-term parked car to a short-term one in the same structure by using the internal power grid; or even transfer power from a group of long-term parked cars to the external power grid when requested to cope with a sudden peak in energy requirements by the grid. In this architecture, data regard both consumption and billing, but are more complex than those of a home consumer as they imply a pro-sumer behavior. As a sample scenario, a charged car may be parked in a structure to stay for a while. During the stay the battery of the car can be drained partially to recharge other cars and hence acting as a power provider, and will be itself recharged only when the car owner shows up and checks out. At this moment the owner must be guaranteed to find the same level of charge in the accumulator or even a higher level more as a payback for the battery wear occurring due to the drain/load operations. In case of an early checkout, the customer should be able to have his car readily recharged possibly at a different cost covering up the service of an earlier recharging.

C. *Multimedia Streaming Scenario*

Multimedia Streaming involves all the actors and has all the services of smart metering (see before). It is aimed at distributing streaming multimedia contents however, in most cases by sharing them locally (e.g., in a house) or by downloading them from a provider/distributor to a consumer. One may think for instance of a multimedia storage and playback digital entertainment console endowed with network connections, including a few power line ones. The large bandwidth provided by power line network connections would allow the prompt delivery of the digital media contents, which could also be exploiting the already existing security measures employed in smart metering to protect the digital goods.

V. Security and Privacy

I Security requirements for the illustrated scenarios can be defined in terms of the three fundamental properties warranted on the data by secure systems: confidentiality, integrity and authentication. Confidentiality implies that a data stream, being sent from an actor to another, should be readable only by the actors involved in the communication, and should not be eavesdropped by anyone else. This property can be warranted by means of tamper proof communication endpoints, to avoid eavesdropper devices insertion, and through employing symmetric cryptography to avoid possible eavesdropping on the communication mean. Integrity regards the necessity that the transmitted data should be delivered to the recipient in whole and unmodified. Integrity may be warranted via a tamper evidence mechanism, such as a message digest, coupled with an on-failure retransmission protocol. In order to properly warrant integrity, the message digest should change radically even when parts as small as a single bit of the transmitted message are changed, and it should be computationally unfeasible to forge a message with a valid digest, different from the original one. Authenticity regards the possibility of identifying either the author of a data block or, analogously the identity of the other endpoint of a communication. The most common means to enforce authenticated communications and authenticate data is to employ asymmetric key cryptography coupled with a Public Key Infrastructure (PKI) able to certificate the authenticity of the public key. Through these means it is possible to provide a secure, mutually authenticated communication between two entities, or to digitally sign data and applications, so that their authorship is undeniably traceable. We now delineate the challenges and technical means involved in providing these fundamental security properties in the three aforementioned scenarios.

A. Smart Metering

The security requirements of the services involved in smart metering basically concern the access permission to a service and the related access mode, e.g., read, write, etc., as well as the classical information security properties like confidentiality and authenticity. These properties provide guidelines on how the various actors communicate over a channel, and how they store information in a database (where it exists – typically at a provider site). Long-term data storage ought to be restricted to the provider only. The energy provider is considered to be a trusted authority, able to keep its own perimeter free from attacks. Security issues may arise when considering inter provider adversarial relations, where a provider may cheat spoofing the others' identities to obtain economic gains. However, since the providers' reputation is effectively a company asset, such threats are not likely to transform into practical attack actions. As providers should be able to intercommunicate among them, a proper structure must be deployed to render the asymmetric key infrastructure interoperable among all of them. To this end, either a common PKI should be instituted among them, or each energy provider should accept certificates signed by the others. Analogously the DSO should be regarded as a trusted entity. Since it is difficult to access the power distribution structures, the security threats concerning the tampering with their metering and information concentration infrastructure receive implicit mitigation by the safety measures included in the step-down power stations where they are placed. On the other hand, since the communication with the power meters happens through the power line, such a connection has to be secured properly. Basically the threats to a DSO are related to network attacks against the flow of data from meters and towards upper levels: user impersonation, rogue server hijacking the traffic, and denials of service caused by artificial message floods. This threat class is the one commonly associated with the communication and application network protocols security issues. Most of the threats are on the consumer side. The consumer may in fact try to lead an attack against the meters. Typically such attacks are of the following types: physical tampering, side-channel analysis, network attacks against the flow of data towards upper levels, user impersonation, connection hijacking. Also, eavesdropping attacks may cause a privacy loss in case a customer is able to gain information regarding the behavior of other ones. Authentication must be provided for the meters that have the ability to detach the consumer from the energy providing grid, in order to prevent the unauthorized detachment of a single consumer or even a large scale intentional blackout targeted to cause massive disruption. Data collected from consumers should be aggregated for statistical purposes only, with no access to individual records in order to prevent fine grained privacy leaking consumer profiling. The aforementioned threats may be the result of a direct attack on the DSO infrastructure or, quite more likely, of a manipulation of the metering devices. In this respect, it is fundamental for the DSO to design and deploy secure meters which effectively hinder any possible malicious action by either outsiders or regular line subscribers. This goal can be achieved in two ways: either the DSO considers its own meter as a closed system where no changes to the running software (other than maintenance updates) are made, or the DSO employs the meter as an open system, allowing the customization of particular features by the line subscriber, via ad-hoc designed applications. The first model assumes that the meter is realized as a closed embedded system, and deals with the confidentiality issues relying only on a shared secret with the DSO, which is embedded at manufacturing time. This in turn implies that the security margin provided by the infrastructure is based on the use of symmetric ciphers in order to wholly encrypt all the communications, thus providing complete confidentiality. The software maintenance updates are sent in encrypted form employing the same shared secret, without the burden of a complete PKI. The alternative system implies that the owner of the meters is willing to run foreign, albeit certified, software on his own devices. In order to avoid the introduction of ad-hoc malware similar to recent SCADA-oriented viruses aimed at altering the measurements and/or the billing features, it is thus mandatory to employ a secure authentication infrastructure for the programs. This fully authenticated chain of trust must thus start providing authenticity warranties on the software components from the first phases of the boot, throughout the whole working cycle of the system. As this infrastructure is designed to foster collaboration and interoperability among the software produced by different meter manufacturers and smart grid stakeholders, it would be a welcome development to design common standards and criteria to provide a common platform on which to develop. Similar efforts have already been born, and grown to a mature state for general purpose computing: a known instance of such a consortium is the Trusted Computing Group (TCG), which has built common grounds for personal computing endowed with a secure boot and chain-of-trust, realized through a specifically designed secure hardware module. Analogously to the security issues tackled for the software, it is equally important to address hardware security issues. As a first step, the hardware components involved in a trusted system should be able to mutually authenticate, in order to avoid the insertion of rogue chips, or the bypass of critical validation components. As this is a common practice in unprotected systems, this threat should be properly addressed, as a hardware security breach results in immediate loss of trust for the whole set of software applications running on it. These concerns can be addressed via properly designed secure hardware modules, employing cryptographically strong primitives and tamper resistant enclosures. In addition to the choice of the primitives and the enclosure design, another fundamental aspect to be addressed is to design side-channel attack resistant hardware, since this whole class of attacks is able to breach the security of a device without the need to interfere with its own tamper proof perimeter.

B. E-car

All the threats to smart metering hold for e-cars as well. This is evident in the case of recharging the car at home. The meters located in a rechargeable car concentration area (e.g., within a parking structure or car station) may be able to communicate to one another via a power line or possibly a wireless channel. Such connections are subject to the same threats as those of smart metering, and hence must be protected as well. These threats might actually be even more serious than those of smart metering, due to the significant amount of money that is exchanged in a typical recharging transaction, to the relatively short time this operation may take (e.g., a fast recharge should be carried out in half an hour at the longest), to the high mobility of the involved actors (vehicle and driver), and to the possibility of billing either the vehicle or the driver. Additionally, the confidentiality of consumers' personal data, of consumptions and of points of recharge, must be guaranteed to avoid consumers' identification, localization and profiling. Host and network security are two increasingly relevant concerns in wireless vehicle-to-vehicle and vehicle-to-infrastructure communications as they play a primary role in order to both warrant vehicle safety, and enhance vehicle traffic management strategies thus resulting in an increased travelling comfort for both drivers and passengers. However, any attack on the embedded IT systems and networks implementing those features may have a life-threatening impact: it is thus necessary to take particular care in the development of the security systems which will hinder completely the actions of possible malicious individuals. The most common security threats in this field are represented by message and/or identity spoofing over car-to-car and car-to infrastructure wireless communication channels and to the injection of fake messages in order to simulate the activity of rogue phantom cars, in such a way to cause artificial traffic jams or stop law enforcement pursuers. An equally security threatening action is represented by the effective deletion of in-flight messages through wireless jamming, thus resulting in possible car accidents. Moreover, in-vehicle sensitive data need to be trusted and protected from forgery. This is particularly relevant if car to infrastructure messages are employed by law enforcement forces in order to drive the activity of semaphores during pursuits or if a possible automatic system of precedence yielding is implemented at car level. In this case, an act of forgery of an traffic enforcement message would result in criminals being able to effectively freeze both passing cars and law enforcement ones to escape capture. Another critical aspect of providing a secure infrastructure for collision avoidance in cars is the fact that the authenticity of the position/speed messages broadcasted by the cars should be parsed and analyzed with strict real-time constraints in order to provide a prompt braking response. Timing constraint points to the possible need of a dedicated hardware implementation of signature verification primitive, due to the low efficiency of digital signature algorithms. The development of a dedicated hardware security module to be integrated into an e-car represents an effective challenge to be tackled in order to ensure an effective way of performing security primitives and storing cryptographic keys in such a way that an attacker cannot obtain them either via wiretapping, visual inspection or side channel attacks performed on the digital circuit. A critical point of this aspect is the secure storage of the cryptographic keys, which should be embedded in a proper way into the chip, taking into account that ASIC reverse engineering up to gate level is now viable thanks to technological advancements in chip imaging techniques. Moreover, in addition to the in-module security, it is fundamental to take into account that the aforementioned secure module does not live in a world of his own: securing the communication of the module with the rest of the embedded hardware is as important as securing the module itself. In this respect, the confidentiality and integrity of the module communication must be warranted, and the mutual authentication among components should be ensured lest malicious ad hoc designed components be inserted in the trusted system to thwart its functionality. In addition to security concerns, the development of intelligent transport systems (ITS) poses new challenges in the field of warranting the privacy of both the owners and the passengers of the vehicles. This concern spurs from the fact that even the basic ITS infrastructure relies on the manipulation of fine-grained and real-time position data of the vehicles, and thus of their owners. This in turn implies that, in a poorly designed system, the geo-localization of the owner could be exploited for any kind of malicious purposes, from stalking to deliberate hindering of the movements of the person. In addition to unlawful purposes, even legally authorized entities could misuse the data they are entitled with in order to obtain economic benefits. A typical case where these issues arise is the one of the automatic, and wishfully anonymous, billing for motorway tolls. In this case, the transaction should be both trustworthy, to ensure prompt payment, and un-linkable with the either the car owner or the driver identity. A promising cryptographic solution in this aspect is represented by zero knowledge proof based protocols, which are able to provide a proof of the possession of a secret token without disclosing it.

C. Multimedia Streaming

All the attacks of smart metering may occur in the multimedia streaming as well. This is mainly due to customers willing to avoid paying for the delivered multimedia content either through skipping the billing phase, or via billing some other customer for their content. Moreover there are attacks to the confidentiality and integrity of large volumes of application data, in the case such data are copyrighted. These attacks are usually targeted at cloning the protected digital content illegally, or at altering certified applications in such a way to remove Digital Rights Management restrictions.

VI. Services

In the following tables, we will list the services provided by the various identified actors of the power grid. Security-related services are in italics. The label “data” refers to both Consumption and Technical data, unless differently specified. Services are reported in verb-noun form. Table I reports services related to the Meter actor, Table II those of the FC, Table III those of the DSO and Table IV those of the ESP.

TABLE I
METER ACTOR AND RELATED SERVICES

basic meter	compute and transmit billing data
	compute and transmit consumption data
	profile consumptions
	report consumption and billing data to FC locally or to DSO / ESP remotely
	manage data confidentiality, integrity and authentication (for data completeness, correctness and integrity)
	ensure tamper-evidence and tamper resistance hardware
	initialize crypto keys and / or certificates
router	routing to manage a home network (on power line and / or wireless)
advanced meter	same services as basic meter and router
	programmability (e.g., upload certified applications)
	trusted computing base – TCB or Trusted Execution Environment

As reported in Table I the basic meter will only need to perform secure actions to manage the data confidentiality during the transmission to the DSO. The rest of the security margin of the meter actor is warranted by the tamper proof encasing which can be endowed with opening detection sensors. Moreover, the secret keys employed for the communication should be properly stored in a volatile memory which can be erased upon intrusion in the meter box. In addition to the tamper proof casing and secure storage of the keys, the meter should also be designed in such a way that it is not possible to extract the secret keys via measuring environmental parameters and exploiting the measures to conduct side channel analyses. The advanced meter, which may extend its functions to a home gateway should also include a full trusted computing base compliant system. The inclusion of a full infrastructure able to run trusted applications is justified by the offered programmability service. Since the possibility of adding custom programs to the meter/gateway implies that it is not possible to perform building-time certification of the programs, the need for the full trusted computing platform is justified.

TABLE II
FC SERVICES

open / close the utility provisioning contract
configure the home network (add / remove program, start-up / shut-down appliances)
request to the meter a report (basic billing or network status or appliance status and consumption)

The FC is able to access services via the facilities exposed from the smart meter. In particular, since the smart meter is running trusted software from the DSO and the ESP, the client can safely update the state of a provisioning contract without the need for extra paperwork. Moreover, in the advanced smart meter, the FC is also able to poll the meter in order to understand the distribution per-appliance of the power consumption of the his house. Another service performable, thanks to the ability of the meter to communicate with other appliances, is to schedule the operation of power demanding appliances in time zones when the cost of the energy is lower, such as nighttime.

TABLE III
DSO ACTOR AND RELATED SERVICES

single consumer or group, e.g., those living in a city area	measure
	profile load
	report consumers’ groups
	aggregate data for profiling
	control meter (e.g., diagnosis, etc.)
	ensure tamper-evidence and tamper resistance hardware
	manage confidentiality, authentication, and integrity of the data received from and sent to meters
	manage the privacy of profile (aggregated) *data*
	initialize crypto keys and / or certificates
group of appliances (group of appliances of the same type, e.g.: e-cars)	report consumptions by consumer or typology (e.g., private user, company, department store, appliance, etc)
	control appliances (hours, times, tariffs, etc) with policy to solve

	conflicts with FC
	initialize crypto keys and / or certificates

The DSO will provide to the meter, and thus to the FC, the backend for all the services mentioned before. Consequentially, it should be able to perform periodic diagnostic operations on the transmission and distribution lines, employing the technical data collected by the meter in order to diagnose faulty or dissipating lines. Moreover it should be able to propagate the consumption messages to the ESP in charge of billing a specific customer, thus providing data transport support for it. In addition to this, the DSO should be in charge of initializing all the key pairs for the final customers' technical messages, which integrity must be warranted, lest they cheat on the payments. The DSO will also be employing the coalesced consumption data in order to avoid service interruptions due to peak requests by the final consumers.

TABLE IV
ESP ACTOR AND RELATED SERVICES

normal operation on the provider side	manage power or resource in the grid
	bill the FC
	Manage or use a PKI
normal operation on the consumer side	as the meter in a basic mode

The ESP, similarly to the FC, may offer its services only through the support infrastructure provided by the DSOs, since DSOs ultimately act as data collectors and transporters. Normally, the behavior of the ESP only takes care of the billing and contract stipulation activities. During these activities, it may be required to set up an ESP bound PKI in order to be able to digitally sign invoices for the final customer.

A. *E-car Scenario*

Theservices of the E-car scenario are split in services offered/received in two situations: (i) at home, and (ii) in a parking area. E-car is seen as an appliance when at home (i.e., it is monitored or managed by a basic or an advanced meter) as well as a producer when in a parking. In such a scenario, the parking manager acts as a DSO and the e-car acts as a prosumer, therefore it is equipped with a meter (either basic or advanced if programmability is needed).

TABLE V
E-CAR ACTORS AND SERVICES

Vehicle	Buy energy
	Sell Energy
	Authenticate with the DSO
Parking lot operator (possibly a DSO)	Measure the provided energy to the car
	Prepare invoices for client billing
	Aggregate collected data for client profiling
	Manage faults
	initialize crypto keys and/or certificates
	manage confidentiality, authentication, and integrity of the data received from and sent to e-cars

	manage the privacy of profile (aggregated) *data*

B. *Multimedia Streaming Scenario*

This scenario represents what may occur at home or in shared office buildings, where video streaming for instance of videoconferencing need to be kept private. An advanced meter, with ad-hoc programmability features, supports the services in Table VI.

TABLE VI
MULTIMEDIA ACTORS AND SERVICES

acquire (buy) contents over a power line or a high speed connection (wireless, optical, DSL)
distribute contents in the house/office via power line or WiFi
manage set-top-box(es) through a power line (exchange payment data with the set-top-box)
provide confidentiality, and integrity of contents, manage cryptographic keys

The advanced metering incorporating the functionalities of the multimedia console should be able to run complex software and will thus need to provide the hardware features to run a full-fledged operating system. This infrastructure is included in the common trusted computing platform enabled architectures, thus allowing the digital media content provider to enforce the use of a specific certified software in order to access the content.

VII. CONCLUSION

As the need for energy increases constantly, the smart management of power grids has become a prime topic of interest for researchers and industry alike. This paper has illustrated the scopes of the TOISE project in the field of power grids security, has described some scenarios and has presented architectural issues able to ensure privacy and integrity in power grid usage. The overall aim of TOISE is to maintain Europe as a worldwide player in the field of efficient implementation of secure integrated devices, to address the future applications. A large initiative is proposed to align a common position in the area. Several TOISE partners participate to related standardization working groups, and TOISE will allow them to develop and promote European solutions in not-yet harmonized bodies.

VIII. ACKNOWLEDGMENTS

This work has been performed in the context of the ENIAC JU project "TOISE". We wish to thank all the partners for ideas and discussion.

IX. REFERENCES

[1] http://www.tst-sistemas.es/en/rd/toise/

[2] The Smart Grid Interoperability Panel – Cyber Security Working Group, NISTIR 7628-Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements; Vol. 2, Privacy and the Smart Grid; Vol 3: Supportive Analyses and References, National Institute of Standards and Technology (NIST), US Department of Commerce, August 2010

[3] IDIS Association, Interoperability specifications.
[On line] http://www.idis-association.com/

[4] https://www.homeplug.org/www_org/KSurvey/pressrelease_db/13da79144ade02e70aed523b8332288503ef147b/pr_file

[5] PRIME White paper MAC specification.
http://www.iberdrola.es/webibd/gc/prod/en/doc/MAC_Spec_white_paper_1_0_080721.pdf

[6] EU Commission Task Force for Smart Grids (European Commission Energy), EG1: Functionalities of smart grids and smart meters; EG2: Regulatory recommendations for data safety, data handling and data protection; EG3: Roles and responsibilities of actors involved in the Smart Grids deployment; EG4: Smart Grid aspects related to Gas
[On line]
http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm

[7] Federal Office for Information Security (BSI), Protection Profile for the Gateway of a Smart Metering System, [On line]
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile

[8] Garcia, F.D., Jacobs, B.: Privacy-friendly energy-metering via homomorphic encryption. In: 6th Workshop on Security and Trust Management (STM). (2010)

[9] Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., Irwin, D.: Private memoirs of a smart meter. In: 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings (BuildSys 2010), Zurich, Switzerland (November 2010)

[10] Rial, A., Danezis, G.: Privacy-preserving smart metering. Technical Report MSRTR-2010-150, Microsoft Research (November 2010)

[11] Danezis, G., Kohlweiss, M., Rial, A.: Di_erentially private billing with rebates. Technical Report MSR-TR-2011-10, Microsoft Research (February 2011)

[12] IEEE, Smart Grid Initiative, [On line] http://smartgrid.ieee.org/

[13] IEEE Standard Association, IEEE P2030 Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads, [On line]
http://grouper.ieee.org/groups/scc21/2030/2030_index.html

[14] ZigBee Alliance, ZigBee Smart Energy.
[On line] http://www.zigbee.org/

Alessandro Barenghi is a Post-Doctoral Research Assistant at the Department of Electronics and Information of Politecnico di Milano, Italy working on the evaluation of the design of efficient, reliable and secure digital cryptographic devices. He received his Ph.D in Computer Engineering from Politecnico di Milano in February 2011 working on “Developments in side channel attacks to digital cryptographic devices: differential power and fault analysis”. His research interests are in computer, embedded and network security focused on applied aspects of cryptography. He is also working in the field of formal languages and compilers, with focus on techniques for parallel parsing, employing operator precedence grammars.

Guido Bertoni is a cryptographer, part of the security team of the corporate R&D of ST. He obtained a degree in computer science engineering and a PhD from Politecnico di Milano. His research interests are focused on cryptographic algorithms, implementation and secure implementation against side channel attacks. He has been contract professor at Politecnico di Milano and actively participated to different workshop and conferences as CHES and FDTC as member of the program committee. He is co-author of more than 30 papers. He participates in the European Task Force for Smart grid, in the expert group 2 of data security and privacy.

Luca Breveglieri is Professor at the Politecnico di Milano, Italy where he works in the VLSI and security groups. He received his Ph.D in Computer Engineering in 1990. His research is in computer arithmetic and signal and image management. He is also working in cryptography and security: VLSI efficient architectures for innovative crypto algorithms, attacks and protection methods for hardwire crypto systems. His research is also in artificial languages He cooperated with CERN to the FERMI (RD-16) project on reliability of data acquisition systems for physics experiments in high energy. He is co-founder and co-chair of the workshop “Fault Diagnosis and Tolerance in Cryptography”, FDTC. He is in the PC of workshop WAIFI (Arithmetic of Finite Fields). He has several projects with Politecnico di Torino, ST Microelectronics Italy, BULL France, SAGEM France, AMTEC Italy, I2E France, CEA France, and ST Microelectronics Italy on various themes of VLSI architectures for crypto computation.

Mariagrazia Fugini is Professor at the Politecnico di Milano, Italy, where she works in the Information Systems Group. She received her Ph.D in Computer Engineering in 1987. Her research interests are in information systems, data security, E-government, safety and green IT. She participated in several EU Projects (TODOS, ITHACA, F3, WIDE, SEEMP, S-Cube. WS-Diamond, GAMES) working on distributed information systems and security models. She is coauthor of ”Database Security” (Addison-Wesley, 1995), and of several papers on security and information system development. She cooperates with Public Administrations in the development of Services to Employment, of wearable services for risk prevention, and on ”coopetition” in service management.

Gerardo Pelosi received his Ph.D. in Computer Engineering and Information Technology in 2007 at the Politecnico di Milano, Italy where he is assistant professor. He has worked on cryptographic databases and data security and privacy, considering access control and privacy protection in data outsourcing. He was research engineer at the Advanced System Technology Laboratories (R&D), STMicroelectronics working on software design, development and optimization of cryptographic libraries for smart cards. His research fields cover information security and privacy, access control models, models for encrypted data management in relational databases, and secure data outsourcing. He is also active in applied cryptography, including side-channel cryptanalysis, system-level attacks, and efficient hardware and software design of cryptographic algorithms. Other research interests are in designing security support into computer architectures and the logic synthesis of combinatorial circuits.