Toward unified security and privacy protection for smart meter networks

DOI:
10.1109/JSYST.2013.2260940

Document Version
Accepted author manuscript

Toward Unified Security and Privacy Protection (USaPP) for Smart Meter Networks

Georgios Kalogridis*, Mahesh Sooriyabandara*, Zhong Fan*, and Mustafa A. Mustafa†

***Abstract*—The management of security and privacy protection mechanisms is one fundamental issue of future smart grid and metering networks. Designing effective and economic measures is a non-trivial task due to a) the large number of system requirements and b) the uncertainty over how the system functionalities are going to be specified and evolve. The paper explores a unified approach for addressing security and privacy of smart metering systems. In the process, we present a unified framework that entails the analysis and synthesis of security solutions associated with closely interrelated components of a typical smart metering system. Ultimately, the proposed framework can be used as a guideline for embedding cross-domain security and privacy solutions into smart grid communication systems.**

***Keywords*-Smart metering security, smart metering privacy.**

I. Introduction

SMART metering (SM) is an important and essential component of the upcoming new power network, smart grid (SG). SM can be defined as the communications hardware and software and associated data management system which allows collection, processing and distribution of information between smart meters, customers and utility companies [1]. The importance of SM is that it interconnects and supports the integration of SG components and functions within a two-way communications network. The objective is to support an economically efficient sustainable power system with high quality and security of supply. This can be achieved with the support of advanced SM functions including automated meter reading (AMR), distributed energy storage (e.g. in Electric Vehicle, EV), distributed energy resource (DER) management (e.g. from renewable resources), and demand response (DR) mechanisms, including incentive-based direct load control, real-time optimisations for load shifting/scheduling. Ultimately, SM will help SG stakeholders to innovate and improve grid operations, optimisations and services.

It emerges that SG and SM systems are underpinned by the utilisation of information and communication technologies (ICT). This exemplifies the increasing dependency of the society on complex systems combining power and automated control systems, communication networks, and computer applications. However, while SG systems provide clear advantages, the dependency on ICT gives rise to vulnerabilities and cyber attacks with potentially devastating results [2].

*Toshiba Research Europe Limited, Telecommunications Research Laboratory, 32 Queen Square, Bristol, BS1 4ND, UK.
†School of Computer Science, The University of Manchester, Oxford Road, Manchester, M13 9PL, UK.
*{george, mahesh, zhong.fan}@toshiba-trel.com
†mustafm@cs.man.ac.uk

Risk analysis and impact assessment is a step towards securing (or upgrading the security of) any system. The application of such a process is non-trivial in a SM network, considering its architectural complexity and interfacing with cyber-physical SG functionalities, and the scale of the potential damages caused by attacks. For example, protection against unauthorised access and repudiation is a vital requirement for the AMR data to be trusted by both the utility providers and the customers. This requires end-to-end communications security, tamper-proof hardware/software and complex access control.

Data privacy concerns the security of data that is linked with, or infer information related to, the life of individuals. The problem of privacy protection is intrinsic in SM because frequent data collection from smart meters reveal a wealth of information about residential appliance usage. Information proliferation and lax controls combined with granular smart meter data collection create a risk of privacy invasions.

Our Contribution: In this paper we introduce a unified security and privacy protection (USaPP) framework that helps analyse fundamental problems of SM security and privacy and search the solution space of security controls in a methodical and holistic manner. Providing a comprehensive security analysis of SM from different stakeholders' point of view is not the objective of this paper. Instead, this study provides an overview of user-related problems and solutions as the basis for suggesting a unified approach. To this end, the main objective of this work is to support the premise that the USaPP approach is vital for sustainable cyber-physical security and privacy management of SM systems, and in general SG systems and complex critical infrastructures. As an example application, we study the security and privacy of an EV dynamic charging use case and apply USaPP solutions.

We organise our material as follows. Section II describes a typical SM system architecture, §III makes an overview of SM security and privacy problems, §IV supports the rationale of USaPP benefits and introduces the USaPP framework, §V analyses further the subclasses of USaPP class elements and maps them with security controls, §VI integrates USaPP with a system-level security analysis framework, §VII applies USaPP to an EV charging scenario, and §VIII concludes this paper.

II. SM system description

A SM (communication) system consists of the following components: Smart meter which primarily measures energy consumption; Home Area Network (HAN) which is used for home appliances and devices to communicate; Wide or Neighbourhood Area Network (WAN/NAN) which connects

HAN to control centres (head-ends) and interested parties; and Gateway which interconnects HAN with WAN/NAN. Fig. 1 shows the typical SM architecture that is being reflected in different USA and European standards such as ZigBee, and ETSI Machine to Machine (M2M) [3].

Optionally, home automation, Home Building Energy System (HBES) and Home Energy Management System (HEMS) may also be connected to the HAN and interface with the smart meter or Gateway. An In-Home Display (IHD), often called the Customer Display Unit (CDU), is a special device that displays data received from the smart meter and optional sub-meters attached to specific appliances, so that a number of home sensors and actuators can be brought together to control and optimise energy consumption. This functionality may further be used to optimise renewable power generation and reach carbon savings targets.

There are a number of options available for the communications outside the home, e.g. between the metering Gateway and the power distribution network, utility or operators. These include cellular technologies, Wireless Mesh/Sensor Networks (WMN/WSN) and various home broadband solutions. However, it remains to be seen if utilities and grid operators will be willing to trust the reliability and independence of some networks. It is more likely that a mixture of technologies will be used. For example, data concentrators/aggregators may collect data from home gateways via wireless networks and then send them on to the utilities through fixed line communications.

Two main objectives of SM is to improve *demand side management* (DSM) and *demand response* (DR) in order to help cut energy costs and adapt to the variability of renewable power generation. DSM involves giving customers financial incentives to shift demands (increase elasticity of demand) as required by the utilities. DSM can effectively be implemented by collecting and analysing customer energy data, making energy saving suggestions, and applying real-time pricing. DR, on the other hand, involves direct control of customer consumption in order to apply peak demand shaving and uses SM to remotely control (e.g. switch on/off) home appliances. The keen reader can find a good overview of DR/DSM functions in [4].

III. Security and privacy issues

A. Related work

While the focus of our paper is not an exhaustive survey of various security and privacy mechanisms of SG, we briefly mention below some of the related work. For a comprehensive review of different security and privacy issues and solutions in smart grid, please refer to [5].

One of the earliest papers that point out important challenges of security and privacy in SG is [6]. The NIST document [7] summarises nicely the security requirements of smart grid and lays out path to standardisation of security solutions. The authors of [8] discuss several key technologies of smart grid, in particular, PKI and trusted computing tailored specifically to smart grid networks. A reliability perspective of smart grid is elaborated in [9], where a systematic and architectural approach is advocated for integrating the diverse IT technologies to realize a reliable, secure, and smart power grid. This, in fact, coincides with the motivation of this paper in which we aim to provide a holistic framework for smart metering security and privacy.

B. Fundamental security problems

SG/SM cyber threats, such as the Stuxnet worm, have the potential to breach national security, economic stability and even physical security. Power stations and SCADA systems have always been targeted by hackers; the move from closed control systems to open IP networks opens up a new range of vulnerabilities. As previously stated, the study of SM/SG security is out of the scope of this paper. The keen reader may refer to the NIST guidelines for SG cyber security [7]; these provide a good starting point and a foundation for SG security analysis, including security attacks, vulnerabilities, risks, requirements, solutions, and research problems. Also, a comprehensive specification of SM security requirements has been published by OpenSG [1].

This paper focuses on the information security of the home SM system as described in §II. The SM system may be attacked from many different entry points. For example, data integrity and authentication may be compromised through network attacks such as man-in-the-middle spoofing, impersonation, or Denial of Service (DoS) attacks. Similarly, data security may be compromised by sabotage/insider attacks such as viruses and trojan horses. The later threat becomes significant considering the openness of the SM system and its interconnections with different networks such as NANs and the Internet.

Once an entry point is found, it becomes easier for the attacker to cascade an attack down the SM system. For example, compromising the real-time pricing channel may result in energy theft or malicious remote control of appliances. Hence, rigorous hardware/software security is required to ensure the validity of different communicating parties such as head-ends and smart meters. Further, consider an attacker takes over the head-end and sends all meters a DR control message to interrupt supply. The interruption can be made permanent by also commanding all meters to change their crypto keys to some new value only known to the attacker [10]. The impact can be enormous: millions of homes are left without power until they are locally replaced or re-flashed with authentic keys, people suffer, health and safety is jeopardised, businesses lose millions. SM security needs to a) prevent such attacks from happening and b) have a recovery/survivability mechanism in case of (successful) attack.

The communication infrastructures are not the only source of vulnerabilities. Software and hardware used for building SM components are at risk of being tampered even before they are installed. Rogue code including the co-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 allowing outsiders to manipulate the system.

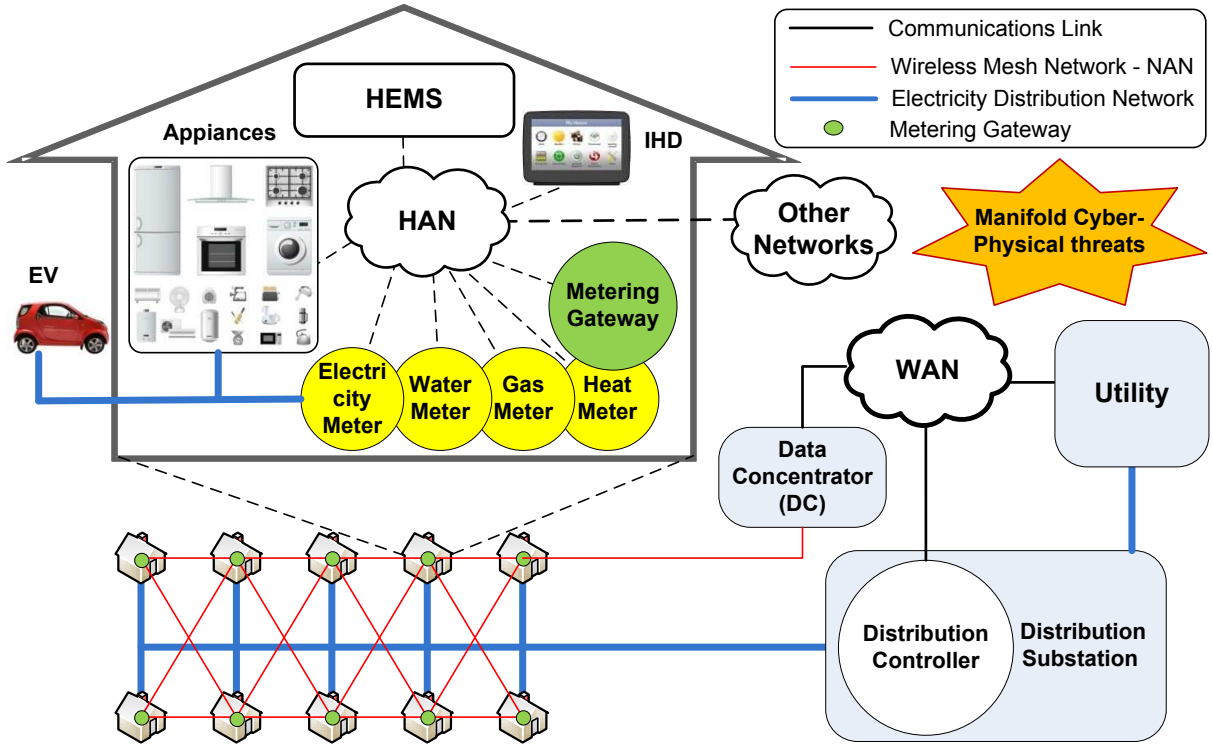

Fig. 1: Typical smart metering architecture.

C. Fundamental privacy problems

The notion of privacy is complex and is perceived and defined in different ways in different countries and cultures. Privacy is associated with the notion of *personally identifiable information* (PII) that may be contained in or linked with certain data. In this direction, we would like to use the notion privacy in the context of the following two notions.

- *Anonymity* is a property of how sufficiently the identity of a user associated with a message is hidden (rather than the message itself).
- *Undetectability* is a property of how a particular item of interest (IOI) associated with a message, is sufficiently distinguished whether exists or not.

The SM privacy problem stems from the potential of a smart meter to measure energy consumption in much more detail than a conventional meter. Smart meters are expected to provide accurate readings automatically at requested time intervals (e.g. every few minutes) to the utility company, electricity distribution network or to the wider SG, to facilitate DSM and DR. Such detailed energy usage can be used to deduce detailed information about appliance usage and lifestyle patterns, as discussed in [11].

The importance of SM privacy and compliance with data privacy regulations has recently been highlighted in the Netherlands, in 2009, where the consumers' association forced the government to back off from smart meter installations until data privacy issues are resolved. According to the Dutch model, SM privacy requires technical specifications and justification for SM data collection and handling and provision of explicit, informed and voluntary consent. Vague assurances of privacy (by the government) are undesirable as they often lead to regulatory capture and irrecoverable data misuse damages. Further standardisation activities in the US and EU involve the development of legal and regulatory consumer privacy regimes that promote consumer access to and choice regarding third party use of their energy data.

IV. The USAPP framework

A. Rationale

Complex critical infrastructure systems which interconnect a number of independent sub-systems to realise new functionality, services and business models could lead to unforeseeable and unanticipated security, safety and reliability related vulnerabilities. Currently a number of international efforts are underway to assess and implement guidelines and methodologies for security and resilience of communications networks and information technology (IT) systems for SG. However, SG is not the first complex system to utilise ICT systems. There are many different example applications in retail and financial sectors which have a wealth of experience in utilising ICT in complex systems. The observation and experience from these sectors indicate that security related to ICT systems have been moving away from conventional layered security concepts towards more systems approaches.

There are many drivers behind holistic system security approaches; some technical and others policy and regulation related. On the technical side, intra-domain security measures are not sufficient to address system level threats. This often raises the need for a unified approach to analysing, implementing and managing security at system level. Such unified

approach provides many benefits during various stages of life cycle of the system; from planning to design, through to implementation and operation. In the planning and design stage, organisations often have to consider legislative, standards-related, regulatory as well as system/application details, including other guidelines and best information security and privacy practices. When developing system security and privacy by design specifications, a decision has to be made about using one or more of domain-specific security techniques in isolation or in combination to develop a solution addressing identified system and stakeholder requirements.

A unified framework such as the one discussed in this paper will help streamline security compliance as well as assist in streamlining the overall space of security solutions. For example, eliminating the use of security schemes which overlap in the solution space can help improve the manageability and reduce complexity without compromising efficiency or security. Further, during system operation stages, unified security solutions can help strengthen security and resilience as follows.

- Preparedness and prevention: the USaPP approach can provide a systematic way of mapping risk and impact assessment results to solutions and (pre-emptively) protect security and privacy by design.
- Detection and response: the USaPP framework can improve traceability by using standardised anomaly detection techniques.
- Mitigation and recovery: the USaPP framework provides a mapping of SG/SM information assets and processes to security controls, which helps segregate safe assets from potentially affected/infected ones and mitigate the cascading attacks due to interdependencies and pinpoint to actions for faster recovery.
- Coordination: the USaPP approach can provide a common platform for international incidence reporting and cooperation.

Whether considering 1) unknown or obscure potential vulnerabilities and weaknesses, based on some dependency analysis and assumptions regarding the maturity level of security controls, or 2) well understood problems that need complex solutions, such as security interconnections among domains and traceability, it appears that a unified system's approach to security is key to methodically addressing the emerging challenges.

Further, it is argued that regulations are not a panacea for customer privacy protection [11]. A holistic approach and application of privacy by design solutions is a *sine qua non* for broad acceptance and success of SGs.

B. Principles

We consider the USaPP framework to be an integrated, holistic approach to the SM/SG security and privacy problems. A unified approach is necessary to study the impact of an SM/SG attacks. This is because SM/SG is a complex physical-cyber system where a vulnerability in one subsystem cascades in vulnerabilities in other subsystems. In non-integrated security systems, complex attacks are typically dealt with by retrofitting obscure security updates. Such problem solving approaches have been proven to be ineffective. For example, IT systems have long suffered from vulnerable security software. Such a lax approach is not prudent for SM networks which is likely to be part of a critical energy infrastructure such as the SG. Instead, a unified approach should be considered from design stage and employed from day one, using open and tested solutions.

From a user perspective, unification facilitates the integration of conflicting SM functionalities and system control at home. For example, energy management and related data flow relationships could be simultaneously applied from different domains such as user, utility and third party energy optimisation agents. Such relationships become more complex as micro-generation and EVs are integrated in home SM networks. Further, USaPP promotes an open market where users change energy supplier, tariffing, energy management contracts, or even control software, on a frequent basis (i.e. daily or less). In such case, both users and stakeholders will need to have a unified way of ensuring that security and privacy is maintained during a 'hand-off' from one (validated) component or stakeholder to another. We note that this paper focuses on the user's perspective.

The integration of security and privacy is also essential. This is because privacy depends on security services such as confidentiality and control. Hence, retrofitting privacy protection mechanisms may be vulnerable if security services are not designed appropriately.

In general, as heterogeneous communication systems converge, SM communications will integrate with ad hoc networks, the Internet, etc. For example, a roaming SG customer may wish to initiate an authenticated flow of information between his home gateway and a remote device. Such data could, for example, be used to authorise access to remote facilities. If privacy is required, the customer may also wish to maintain anonymity. The extrapolation and combination of multi-domain information such as energy consumption data, location information, lifestyle information, and other personal information increase the potential both for richer applications and services as well as security threats and damages. Future integration of systems and services require transparent USaPP by design more than any other time.

The evolution of SM systems also requires scalable and future proof architectures. For example, consider the case where the collection frequency of smart meter data and control functionality change. This change may increase the risk of data privacy infringements and remote attacks such as impersonated control messages. A scalable security system should be able to increase protection levels as required.

C. Framework elements

Given the system requirements outlined in §IV, in this section we propose a USaPP framework with an emphasis on home solutions, as illustrated in Fig. 2. However, we do not preclude the adoption of the proposed framework in a broader SM/SG security system.

We organise SM USaPP solutions in the following three classes.

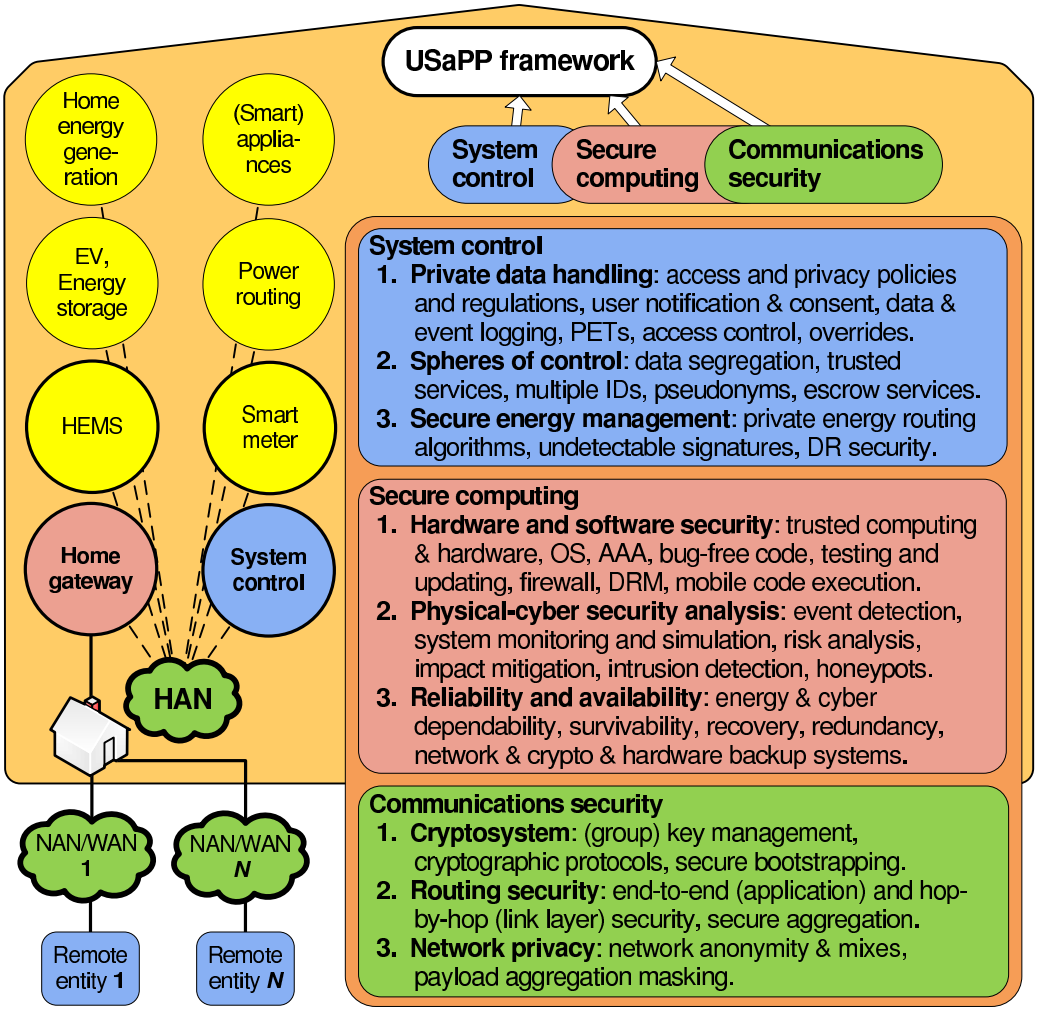

Fig. 2: Unified Security and Privacy Protection (USaPP) framework for home SM systems.

- Communications security. This class involves two distinct communication systems: a) in-home HAN, HEMS, and HBEMS, and b) WAN/NAN, including WMN/WSN.
- Secure computing. This class involves the hardware and software security systems integrated in different SM components that can operate SM system functions such as energy and cyber system control, including communications.
- System control. This class involves the SM functions and the variables (user input, rules, policies or decision making algorithms) that drive computing or communication USaPP operations. This class is responsible for deciding what security services are needed for different functions and where/how different data is protected and communicated. That is, this class is responsible for configuring home SM operations and resolving conflicting requirements (e.g. energy saving vs. privacy vs. user overrides vs. SG overrides).

Each class integrates both security and privacy protection measures and comprises three sub-classes, which are outlined in Fig. 2 and further discussed in §V.

V. A MAP OF USAPP SOLUTIONS

A. Communications security

1) Cryptosystem: Remote access and control within an SM system, such as DR functionality, may involve a) heterogeneous private or public networks, such as the TCP/IP-based networks (Internet) and WMNs, b) many different devices, such as sensors, access points and SMs, and c) different actors, such as utilities and customers. Communications security for such systems entails key management in different security domains. However, all NAN/WAN sensors and SMs of a city may all need to be integrated in a single security cryptosystem involving maintenance of possibly millions of cryptographic keys and other credentials. Hence, SM communications security needs to combine large-scale, economic key management and cryptography that can be carried out effectively on devices with limited processing power.

The design of an SM key management system is an active area of research. This could for example be based on existing systems such as Public Key Infrastructure (PKI) and Identity-Based Encryption (IBE).

In general, a mixture of hierarchical, decentralised, delegated or hybrid security schemes may be feasible. Prefer-

ably, a candidate scheme should include secure bootstrapping protocols, i.e. it should provide effective means to initialise new devices. Further, critical security operations, such as key updates, should preferably employ *group key management* techniques, such as 'defence in depth' techniques used in nuclear or military control systems, to mitigate the impact of compromised head-ends (or trusted people).

2) Routing security: Network routing architecture has an impact on security. For example, consider a NAN implemented using WSN in which a number of intermediate wireless nodes aggregate traffic to optimise bandwidth usage and increase network reliability. If an end-to-end encryption scheme is employed, aggregation can be as simple as concatenation of encrypted data. Alternatively, secure aggregation is feasible using additive privacy homomorphism protocols [12]. End-to-end security ensures that data security services are resilient to compromised or rogue aggregators. Further, link layer (MAC/PHY) hop-by-hop security may be required to protect against DoS attacks such as flooding attacks. For example, 6LoWPAN security may provide some security services such as integrity and authentication.

3) Network privacy: Privacy protection requires standard security services such as confidentiality, authentication and access control. Such security services need to be employed at different SM layers, including communications, storage and computing platforms. However, that kind of measures may not suffice. For example, end-to-end communications security may only guarantee message payload protection. Private information may still be exposed from 'shallow packet inspection' (e.g. analysis of IP addresses), which is feasible in WMNs such as 6LoWPAN. That is, privacy also requires network anonymity, as defined in §III-C. In such cases, possible protection mechanisms include *network mixes* such as *onion routing*.

In a broader SM network system, different gradients of SM data anonymity may be achieved as SM data is cascaded in downstream systems. This can be engineered by effectively removing different degrees of privacy information from SM data in intermediate systems/aggregators. We note that an SM aggregator may also offer undetectability (as defined in §III-C). For example, the superposition of the metered load signatures of (sufficiently) large blocks of homes will effectively reduce the probability in detecting a particular IOI such as the operation of a TV set.

B. Secure computing

1) Hardware and software security: Secure computing solutions involve the protection of programmable hardware components, including software and firmware. Security holes such as backdoors and software bugs may allow hackers to compromise standard cyber security solutions such as cryptographic protocols offering authentication, access control and accountability (AAA).

SM systems may include complex computing platforms such as operating system (OS) running on personal computers. Such devices need to employ well-designed OS/application security architectures such as firewalls, to protect against both malware and poor user practices, such as poor storage of important cryptographic keys, poor user/system trust and password management, and social engineering.

The SM system should be resilient to both insider and incoming attacks from open interfaces and give access permissions to authorised parties as appropriate. For example access rights may be managed by a Digital Rights Management (DRM) system. Also, applications may communicate on complex distributed programming platforms such as mobile agents; this requires suitable mobile code security measures. Finally, the system should be undergoing continuous exhaustive analysis testing, bug fixing and updating.

Certification and accreditation are critical process in guaranteeing HW/SW security. Common criteria (CC), FIPS 140 and PCI PTS are generic certification schemes. Additionally ISA 99 standardises security controls for embedded systems. However, extensions will be required to include security profiles for SM/SG, similar to those related to the smart card industry. Alternative, and quicker, tests include 'white-box' and code audits, employed by the US national SCADA test bed programme. Certification governance may also consider an adaptation of the ISO 27K series of standards, as it occurred with the telecommunications security.

2) Physical-cyber security analysis: A holistic approach should be taken to analyse USaPP of the SM system. For example, SM communications security vulnerabilities can directly compromise billing, HEMS and DR functionalities, and grid stability. Hence, SM security should be integrated to address problems in both the cyber and energy domains. It is particularly important to design a unified intrusion detection system that will monitor and analyse both cyber and energy events, such as potential attacks and impacts. For example, intrusion detection checks may include key management and routing protocol operations, packet headers and payloads, security logs, traffic statistics, wireless signals, system and data integrity. Additionally, *honeypots* may be used to isolate and analyse attacks.

In such complex computing, communications and energy management environment, it is important to simulate risks of the broader SM/SG system. That is, cascaded risk should be evaluated, whereby compromise of one system leads to compromise of a downstream system. A risk analysis model should be able to detect both proactive and reactive system anomalies and take appropriate measures such as create appropriate logs and alerts.

3) Reliability and availability: The reliability and availability of energy, in the physical sense, probably form the most critical security requirements. However, it is wrong to consider data integrity and confidentiality less important, as such security services may be cross-correlated. For example, lack of data integrity may yield unreliable billing. Even worse, compromised data AAA may allow intruders to manipulate SM appliances and even cause physical damages (e.g. one could force the gas heaters to operate on full power), let alone potential greater SG threats such as substation sabotages leading to system breakdown and widespread energy blackouts (which we do not study here).

Reliability can be induced by means of redundancy. One such example is depicted in Fig. 3 where the integrity of

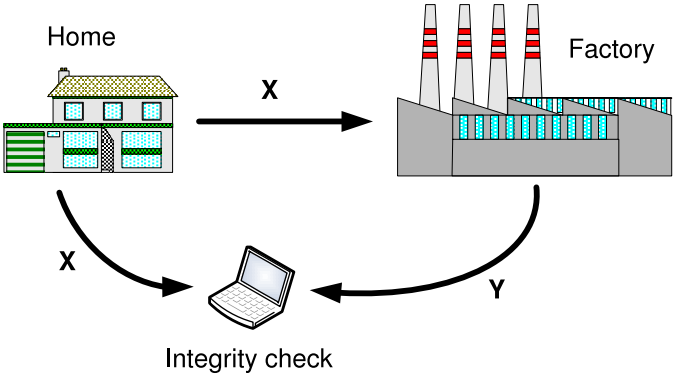

Fig. 3: Redundant measurement system to verify the integrity of the reported measurements.

gathered billing data $\mathbf{X}$ can be verified if an integrity check $\mathbf{Y}$ is fed back to be compared with $\mathbf{X}$. Sending back $\mathbf{Y}$ instead of $\mathbf{X}$ increases the level of security when $\mathbf{Y}$ is sent over an untrusted network.

Survivability functionality needs also to be in place to handle emergency situations when critical security services fail. Solutions may involve the addition of system redundancy functionality such as different ways to access system components. For example, a home gateway may be simultaneously be accessed through different communication networks. Also, critical devices may be accessed by more than one gateways or access points. Finally, multiple parties, such as delegates and escrow services may be used to add diversity in AAA services. In such cases, critical devices may need to maintain multiple (backup) crypto keys.

C. System control

1) Private data handling: Secure data handling requires transparent policies, trust management and compliance enforcement mechanisms. Architectural solutions for data handling include Privacy Enhancing Technologies (PETs), which may employ a variety of cryptographic or anonymity protocols. For example, PETs may be based on standard 'privacy principles' such as notice and purpose, choice and consent, collection and scope, use and retention, access, disclosure to third parties and limited use, security for privacy, quality, and monitoring and enforcement [13]. Access to data should be controlled with cryptographic protocols.

PETs could also be used to assess privacy risks and moderate SM data communication and handling. SM privacy risk may be quantified by analysing the leakage or exposure of PII to different parties. Privacy protection risk assessment depends on privacy parameters such as a) the value of data, b) the ownership of data, c) data access and usage permissions given to different parties, d) the degree data owner trusts such other parties with the data.

Harmonising privacy regulations across different legal systems and cultures is not easy. For example, in the USA there are 51 different standards for privacy: one for each one of the 50 states plus one federal standard. Regarding data ownership, each state has different rules: in some states it is the individual, in some others the electrical company, and in others a third party.

We note that trusting stakeholders for complying with regulations is not a panacea for protecting privacy. This is because regulations are often equivocal and not easily enforced. History (e.g. of Internet) teaches that 'legitimate' data mining and exploitation techniques evolve quickly when there are financial incentives. To overcome this problem it is desirable to define a common, unified language in order to design validated contractual customer-stakeholder relationships in a structural manner.

2) Spheres of control: Spheres of control are useful to mitigate vulnerabilities by giving different levels of control to different trusted parties for different data or functionality. For example, we suggest that private data could be segregated into the following categories.

- Customer data: These could be low frequency attributable data such as data used for billing.
- Technical data: These could be high frequency SM data such as data supporting DR/DSM.
- Strictly personal data: These could be per unit data sampled at the highest frequency used for personal or private business purposes.

The difference between the above categories of data is that each dataset contains different amount of information. That is, customer data will have a low information content while strictly personal data will have a high information content. Thus the leakage of the latter will pose a greater risk to customer privacy.

It becomes clear that empowering the user to control access to granular SM data, including giving consent for access to SM/SG stakeholders, is key to implementing a hierarchical access control system for privacy preservation. For example, the Expert Group 2 of the European Task Force Smart Grids [14] has recommended that technical SM data should be anonymised with means of data aggregation, as discussed in §V-A3.

Apart from using aggregation, data privacy and control may be further advocated with the introduction of trusted third parties, such as escrows. The benefit here is that an independent escrow service allows secure end-to-end aggregation of SM data payloads in a very scalable manner.

An escrow-based anonymisation scheme proposed in [15] introduces a structural difference to a smart meter within which two separate IDs are embedded, as depicted in Fig. 4: one anonymous, High-Frequency ID (HFID) and one attributable Low-Frequency ID (LFID). The idea is to use HFID to send technical data, and LFID to send customer data. The idea here is that HFID will never be known to the utility; however, the utility can verify the integrity and authenticity of associated messages with the help of the escrow.

We note that multiple-ID hardware architectures, as in Fig. 4, may support a) escrow anonymisation discussed here, b) group key management protocols for attack impact mitigation discussed in §V-A1, or c) backup keys trust for emergency hardware control discussed in §V-B3. This again illustrates the importance for having a USaPP design.

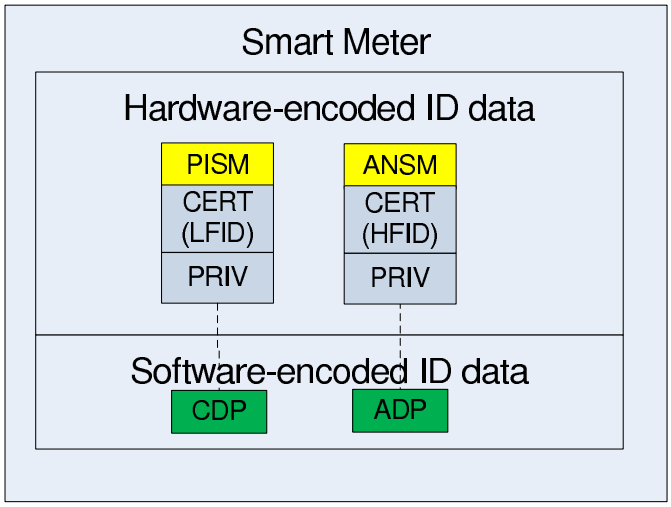

Fig. 4: Smart meter hardware architecture containing a) a Personally Identifiable SM (PISM) Profile and b) an Anonymous SM (ANSM) Profile. Each profile contains: a Certificate (CERT), corresponding hardware ID, Public Key, Private Key (PRIV), and root Certifying Authority (CA) data. The two profiles are used to create or update a Client Data Profile (CDP) and an Anonymous Data Profile (ADP).

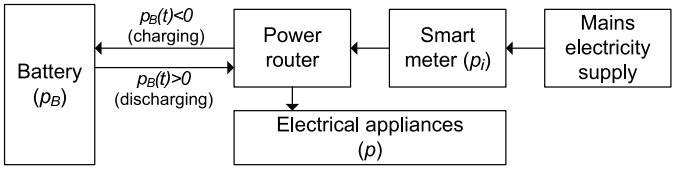

Fig. 5: The battery is discharged/recharged with power $p_B(t)$ in order to 'disguise' a given consumption load $p(t)$. The smart meter records a power trace $p_i = p - p_B - p_L$, where $p_L(t)$ is the power lost within the battery.

3) Secure energy management: The concept of privacy via undetectability discussed in §III-C adopts the fundamental assumption that hiding home appliance usage patterns is a matter of 'privacy of personal behaviour', i.e. "the right of individuals to keep any knowledge of their activities, and their choices, from being shared with others" [13]. In this context, SM privacy can be studied as an undetectability property of appliance load signatures [16]. Undetectability can effectively be enforced by controlling the energy flow within a home so that a portion of a consumption demand runs off a rechargeable battery, rather than directly off the grid, as seen in Fig. 5. The battery system may manage energy flow in a manner advantageous to customer privacy by masking load signatures in a way that makes it harder to detect appliance usage patterns.

From the above it becomes clear that HEMS decision making algorithms can effectively impact SM data privacy. However, the degree to which this it true depends on deployed spheres of control discussed in §V-C2.

It should be clarified that private energy management may conflict with other SM functionality such as DR/DSM or energy pricing arbitrage, and is bounded by the physical limitations of the battery. For example, $p_B(t)$ in Fig. 5 might contain loads that a) have been shifted in an undesirable manner and/or b) reveal some appliance (and battery) usage patterns. The development of optimal privacy preservation and/or cost minimisation algorithms by using a rechargeable battery is a problem of future research.

VI. Security Analysis

A. SM/SG risk assessment

The process of evaluating the security of a system typically involves the specification of (baseline or increased level) security requirements, the identification and analysis of applicable threats and vulnerabilities, and the application of appropriate security controls, such as the ones discussed in §V. Threat analysis, in particular, can be performed following different approaches as follows:

- Top-down approach: threats and vulnerabilities are identified for specific scenarios.
- Bottom-up approach: 'common' security requirements (such as integrity, confidentiality, authentication, accountability, availability, and anonymity) are analysed for the various system components and functions.

The security analysis of complex systems, such as SM/SG, is commonly directed by regulatory frameworks for critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP). One of the key elements of such CIP/CIIP is the application of risk assessment methodologies, including dependability and interdependencies analysis.

Current risk assessments used by DSOs are not good to deal with the very distributed nature of SG/SM systems [2]. This challenge has been recognised by the Smart Grids Task Force (SGTF), set up by the European Commission (EC), and Mandate M/490 Smart Grid Coordination Group (SGCG) and smart grid information security (SGIS) working groups (WGs), which is currently developing a risk assessment toolkit [17].

The USaPP framework neither specifies nor contributes to SM security or risk analysis. Instead, the role of USaPP is standardise and unify a method of methodically identifying security controls within its classified solution space. This will, in retrospect, help perform a methodical risk analysis as this process is underpinned by assumptions regarding existing security controls.

B. System integration and benefits

As previously discussed, the USaPP framework helps map security analysis results (e.g. prioritised security design or update requirements) to security controls. At system level, the integration of USaPP with standard information security management processes can be see in Fig. 6. This system's approach of a holistic security management consists of the following processes.

- Stakeholder analysis: this involves a stock taking of SG/SM stakeholders' development drivers and critical requirements, including policy-driven rulebases, standards'

compliance, market sustainability, and customer satisfaction. This analysis helps formulate a minimal set of high level security and privacy goals.
- Functionality and use cases: functional requirements and specific use cases have their custom security and privacy requirements. These custom requirements become more specific by mapping the corresponding functions and operations into a reference system architecture. Further the importance of these requirements may be filtered by linking them with the high level goals obtained from the stakeholder analysis.
- Risk assessment: the reference architecture can be further used as a basis to identify potential use case threats and vulnerabilities and assess their potential impact to the system. This helps identify the set of security weaknesses that pose high risk and will need to be addressed.
- USaPP solution space: this involves using the USaPP framework to help identify security controls in a unified and systematic manner. This process will be further analysed later on in this section.
- Update mechanism: assuming that a (chosen) security measure is implemented and, thus, the reference architecture is updated, the risk assessment and USaPP application could be performed iteratively to make sure that threats to security and privacy pose a low risk. Additionally, the process is reiterated when a new use case of functionality is inserted, or when the stakeholder goals change.

The process of using USaPP to help organise the search of required solutions is given in grater detail in Fig. 7. This operational methodology comprises the following steps.

1) The system security (and privacy) requirements are identified and grouped for each separate use case.
2) Given a security requirement, security interdependencies are identified across different domains. In SM systems, and in this example implementation, we consider, four distinct domains as in house, DER/EV, distribution, and retail. Further, each domain is further organised in two orthogonal categories. The first one is the physical-domain, which concerns the security of HW components, and the second one is the cyber-domain, which concerns the set of (secure virtual) entities that are allowed to access and actuate on the reference domain (and potentially regardless of their physical location).
3) Given a certain location in the horizontal plane of Fig. 7, which corresponds to a use case requirement for a certain domain category, a designer is expected to search the pool of USaPP solutions, which are grouped into three top-level classes, and further second-level subclasses, as see in Fig. 2.
4) The application of each USaPP (subclass) solution is further broken down into five layers, which namely are: business, function, information, network, and component layer. The business layer corresponds to solutions that involve organisational or regulatory aspects. The function layer corresponds to solutions that involve services and logical processes. The information layer corresponds to solutions for data models and credentials. The network layer represents solutions for mechanisms and protocols that support data communications. Finally, the component layer corresponds to solutions that help protect platforms that host functions, information and network elements. This layered classification is similar to the layers of the European SG architectural model [17].
5) Given that a security requirement for a domain can be addressed by employing a solution in a interdependent layer of the SG, the systematic reduction of the search space facilitates a rigorous and efficient search.

Given the above methodology, it becomes clearer that the benefit of USaPP is that it helps eradicate fragmentation in the application of security measures, which has traditionally been based on the insightful considerations of security experts. The proposed USaPP classification helps specify a minimum set of standards and regulatory mechanisms by mitigating duplicating security services of overlaying security controls. A minimum set of standards will concern a common/unified reference architecture and common security management processes. This helps justify the premise that USaPP is advantageous as compared to standard security mapping methods as it improves interoperability and standardises security analysis. Further USaPP could provide a common platform for national coordination e.g. through computer emergency response teams (CERTs).

VII. Case study: EV charging security

This section presents an EV charging case study to demonstrate how the USaPP framework can be applied to address the security and privacy issues in a SM/SG application.

A. Controlled EV charging

Electric Vehicles (EVs) are envisioned to be an integral part of the future SG. This is because, in addition to functioning as vehicles, they can also be used as a) storage facilities for any surplus electricity (e.g. electricity generated by intermittent renewable sources), and b) distributed energy resources when they discharge their batteries and feed electricity back to the grid [18].

However, letting users to recharge their EVs in an uncontrolled manner could endanger the stability of the grid [19]. To prevent this, or to reduce the chance of destabilising the grid, EV chargings should be done in a controlled (coordinated) manner [4]. For example, EVs should be recharged when the grid is lightly loaded and/or when there is surplus electricity. In order to influence the times when users recharge their EVs, some price-driven incentive-based DR mechanism could be put in place, e.g. adaptive electricity pricing that changes depending on the current state of the grid; examples of such pricing mechanisms include real-time pricing, time-of-use, critical peak pricing, etc.

In addition, grid operators would offer payments for providing ancillary services to the grid (e.g. frequency regulation, demand response, spinning reserve, etc [18]). EVs are suitable for offering such services due to their fast reaction capabilities.

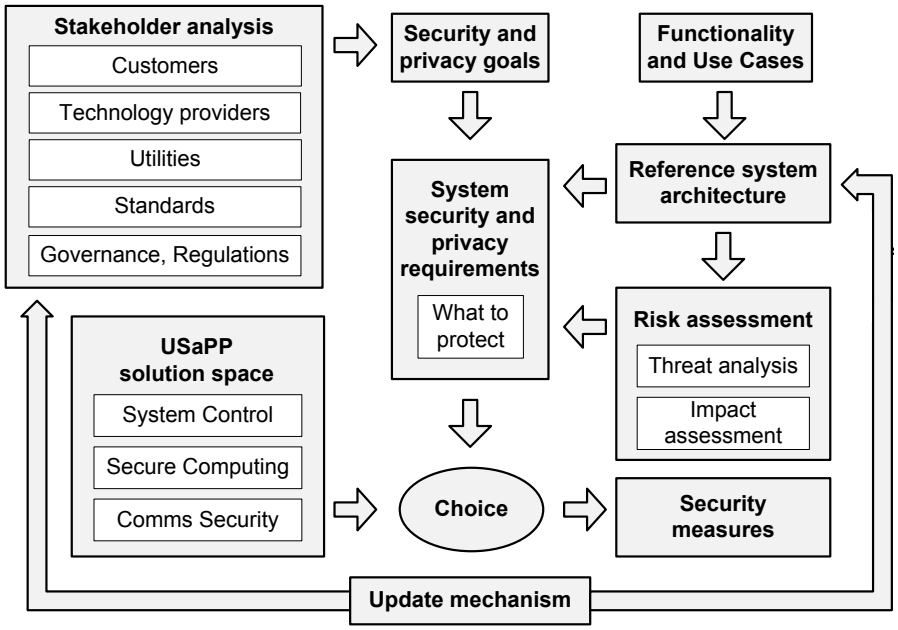

Fig. 6: USaPP system integration.

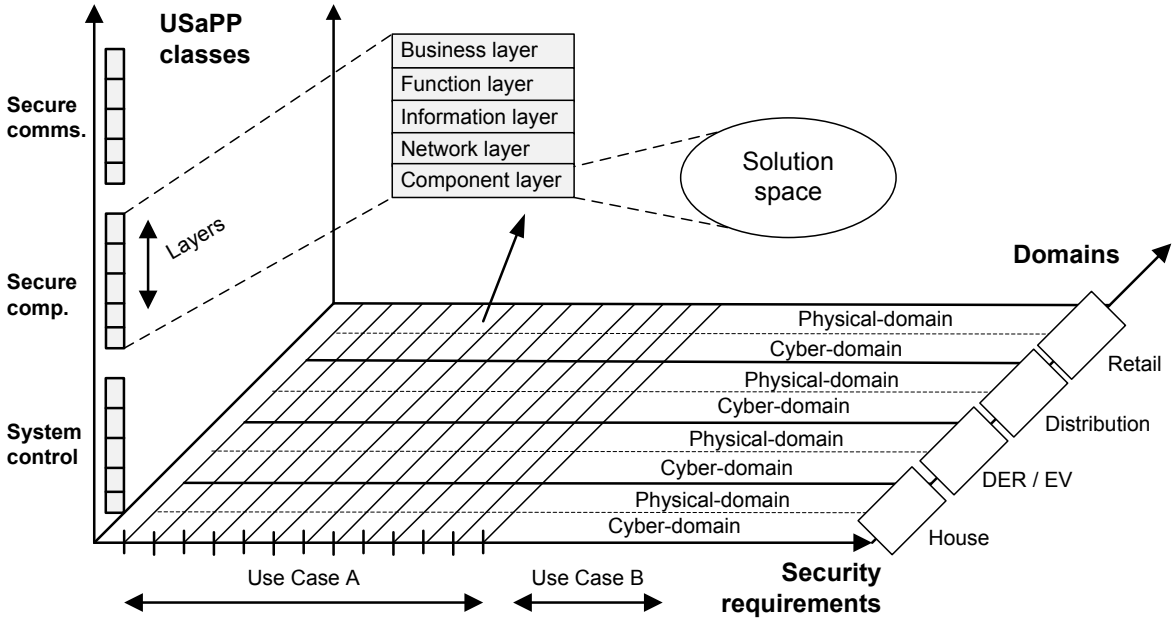

Fig. 7: USaPP operational methodology.

However, to be eligible, an ancillary service provider has to be able to offer at least a certain amount of flexible demand. As an EV typically has a limited battery capacity, there is a need for a new entity, EV AGGregator (EVAGG), to be created. EVAGG will aggregate the batteries of a number of EVs and represent their users in the electricity market, i.e. it will act as a middleman between users and grid operators. Fig. 8 illustrates the necessary interactions among entities involved. More precisely, if an EV user agrees to offer ancillary services to the grid, the EV's battery will be added to the EVAGG's aggregated load. With this flexible load, the EVAGG could bid in the electricity market for offering ancillary services. If the bid is accepted, the EVAGG will receive instructions from the grid operators to adjust its load. To comply with the instructions, the EVAGG may change the charging process of some of the EVs (e.g. adjust recharging levels, terminate recharging, commence discharging, etc) by sending Control Signals (CSs) to some of the EVs. In return, for the load provided, the grid operators will pay to the EVAGG which will, in return, pass on some of the payment to the EV users. This is another mechanism to incentivise users to charge their EVs in a way that it would bring benefits to all parties concerned.

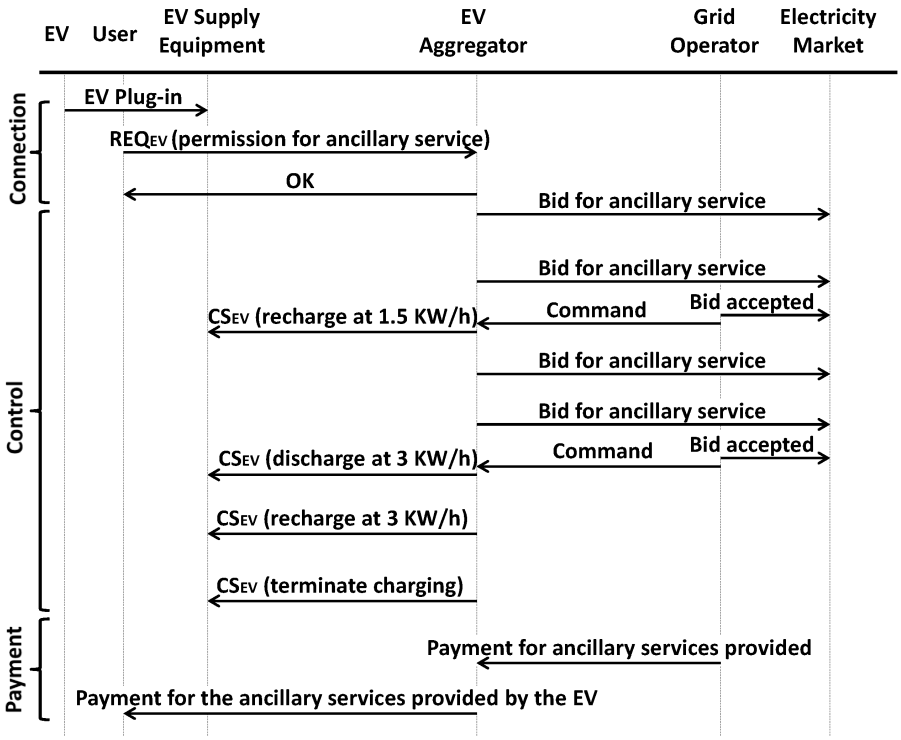

Fig. 8: EV used as an ancillary service provider via EVAGG.

B. An exemplar EV charging scenario

Fig. 9 illustrates one of several possible EV charging scenarios. Here it is assumed that user B (Ub) visits user A's (Ua) home and charges his EV (EVb) on the premises of Ua. Ua and Ub have contracts for electricity supply with utility companies, utility A (Uta) and utility B (Utb), respectively. Ub also has contract with EVAGG for offering ancillary services. It is assumed that Ua has Renewable Energy Source (RES) on her premises.

Depending on the amount of electricity generated from RES, during recharging, EVb may just get electricity supplied by the RES (if RES has sufficient stock), by the grid (if RES has zero stock), or by both RES and the grid (if RES has some stock but not sufficient for EVb's demand). Depending on these different situations, the payee of Ub's payment and the amount payable to the payee may vary as well. In other words, Ub may need to pay for the electricity to Ua, to Uta, or to both of them.

Similarly, if EVb is discharging, depending on the Ua's current demand for electricity, the electricity fed by the EVb could be used by Ua's home appliances, be fed back to the grid, or some used by Ua's appliances and some fed back to the grid. Depending on the different cases, Ub may be paid by Ua, by Uta or by both of them. In addition, Ub may also receive payment from EVAGG for any ancillary services provided by the EVb to the grid.

Moreover, the time, level and continuance of the charging may also depend on a) user's preferences, b) available electricity generated by the local RES, c) the current price signal, d) the state of the distribution networks, e) any CSs sent by EVAGG, etc.

C. Addressing security and privacy issues using USaPP

In the example above the charging of EVs requires the involvement of multiple entities and potentially complex interactions. For example, Uta would need to deliver the current electricity price to Ua and also access her meter readings (for billing purposes), EVAGG would need to have real-time communication with EVb to obtain data about its battery's current status (to be able to use EVb as an ancillary provider), distribution network operators would need to access meter readings of Ua (to be informed about grid's overall demand), etc. Such a complex process not only introduces a large number of security and privacy concerns, but also dictates that the approach to the security and privacy concerns should be structured, integrated and unified.

For example, adversaries may try to impersonate different entities (e.g. Uta, Utb, EVAGG, etc.), eavesdrop and/or tamper with the messages (e.g. pricing signal, CSs, etc.) communicated in EV charging sessions to attempt to destabilise the grid. This could lead to disruptions of electricity supplies and even threaten the national security of a country. From the privacy point of view, knowing an EV's identity, its location and its user's identity may be sufficient for a perpetrator to profile an EV user or to prepare for a further attack in the name of the user.

To analyse these threats, we need to identify the interactions and entities involved, thus addressing the key management issues ensuring the right keys are shared only among authorised entities. As IBE allow devices with low computation power to start sending messages without a need to contact a key server, IBE is one of the strong candidates for being deployed in SG/SM systems. In addition, we also need to consider

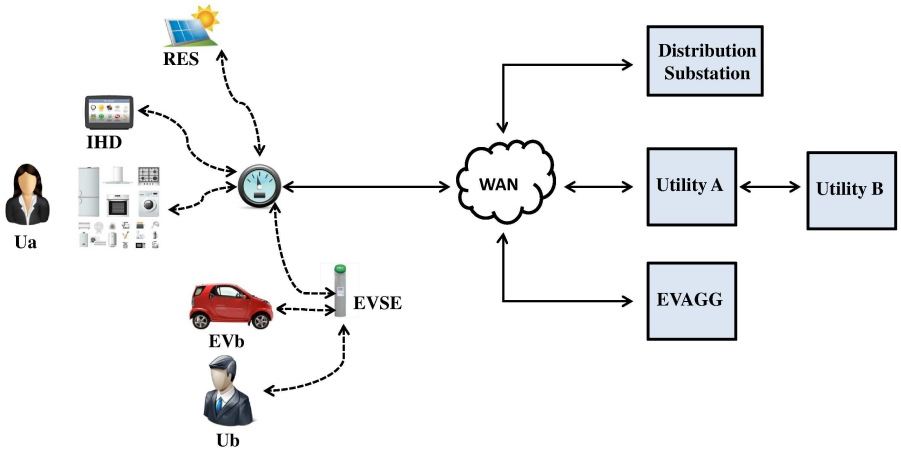

Fig. 9: A roaming EV user at a typical home of the future.

routing security, and secure data aggregation to corroborate the confidentiality of SM data. In addition, EVb electricity consumption data measured at EVSE would be communicated to Utb and EVAGG (for billing purposes), and EVAGG would be sending CSs to EVb. As these data are directly related with the current charging session, secure end-to-end and peer-to-peer basis communication would be more appropriate. If Ub wishes to preserve his location privacy, i.e. wishes to hide the fact that he has ever visited Ua's home, then network privacy techniques should be considered such mix-networks, onion routing or anonymisers.

Other types of threats to the EV charging include legitimate but not genuine data or commands sent by different entities. For example, incorrectly executed optimisation of EVs' charging schedules could trigger an EV to start recharging at peak times causing financial losses to its user.

Furthermore, protecting EV users' privacy is a challenging issue. In the context of this scenario, privacy related scenarios can be follows: 1) Ua may not want to reveal to Uta that there is an EV (in our case EVb) using the charging facility; 2) Ub may not want to reveal his identity or EVb's identity and EVb's electricity consumption to Uta or unauthorised eavesdroppers; 3) Ub may not want to reveal identity and EVb's identity to EVAGG, but still act as ancillary provider and get payments for offering this service.

To address these privacy issues, different methods can be employed. For example, in the first scenario a secure energy management mechanism can be deployed by managing EVb's recharging process in a way that it mimics electricity usage of standard home appliances. In such way, Uta would not be able to detect the presence of any EV charging processes. In the second scenario Ub's anonymity can be provided by employing trusted third parties or pseudonyms. However, anonymity may not be sufficient to prevent adversaries from linking together EVb's multiple charging sessions. The non-linkability property can be achieved by assigning a dynamic identifier to each of the charging sessions performed by Ub. Of course, a controlled and authorised linkage of Ub's multiple charging sessions should be supported, to ensure accountability and traceability in the event of a dispute or security incident. In such way, EVAGG would only need to know the anonymous Ub's contracted utility company (Utb) in order to make payments to Ub (via Utb) and request Ub's real ID revelation in case of disputes (solution for scenario three).

Table I lists some potential EV charging security issues and categorises them into the classes of the USaPP framework.

D. Importance of USaPP

From the EV charging scenario analysis above, it would appear that the USaPP framework is useful in providing a systematic way to identify and classify a number of security and privacy issues as in Table I. Such a classification would help designers to explore better the pool of existing solutions. For example, the false control signal, false price signal and false network status signal issues could be addressed by the same or similar solutions.

Without applying USaPP, it is likely that designers would provide solutions to different issues, and these solutions may not integrate with each other. Therefore, new solutions should be planned and designed in a way that they do not overlap or conflict with solutions that address security and privacy issues belonging to different classes.

Using this systematic way of tackling different subcases could increase the efficiency and reliability of the entire design and launch cycle of products related to the EV charging application.

VIII. Conclusions

The interconnection of cross-disciplinary systems, such as HEMS, HBES, HAN and WSN, the need to collect and analyse detailed SM data, the support for various SM functionalities, such as real-time pricing, DR and DSM, and the involvement of multiple stakeholders (e.g. consumers, utilities, grid operators, third-party service providers) make SM systems highly complex. Equally complex is the analysis of security and privacy attacks that may cascade from one SM system domain into another. In this paper we have presented the case for a unified approach that attempts to address home SM

TABLE I: EV charging security issues.

EV charging	Communication security	System control	Secure computing
False control signal	x	x	
False price signal	x		
False optimisation method		x	x
False network state signal	x		
Software bugs		x	x
Malicious software on OS		x	x
Bugs in cryptographic protocols	x		
Poor storage of cryptographic keys			x
Replay attacks	x		
DDoS attacks on EVAGG	x		
Lack of user/EVAGG accountability		x	
Disclosure of sensitive data	x		
Privacy breaches (user ID, EV location)	x		x

security and privacy requirements by fusing different solutions and mapping them to a number of tightly inter-related system components. In particular, by classifying discussed solutions into three logical domains, namely, communications, computing and system control, the proposed USaPP framework addresses the SM network security and privacy issues in a holistic manner. We believe that the proposed USaPP framework can be used as a guideline for SG network designers and the future work will focus on many of the technical solutions embedded in different domains of the framework.

ACKNOWLEDGMENT

The authors would like to thank the Directors of the Toshiba Telecommunications Research Laboratory for their support, as well as Dr. Tim Farnham for his invaluable comments.

REFERENCES

[1] B. Brown, B. Singletary, B. Willke, C. Bennett, D. Highfill, D. Houseman, F. Cleveland, H. Lipson, J. Ivers, J. Gooding, J. McDonald, N. Greenfield, and S. Li, *AMI System Security Requirements*, December 2008, AMI-SEC TF, available at http://osgug.ucaiug.org.

[2] ENISA, *Smart Grid Security: Recommendations for Europe and Member States*, July 2012, available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations.

[3] ETSI, *Machine-to-Machine communications (M2M); Smart Metering Use Cases*, May 2010, TR 102 691, v1.1.1, available at http://www.etsi.org/deliver/etsi_tr/102600_102699/102691/01.01.01_60/tr_102691v010101p.pdf.

[4] E. Lu, D. Reicher, C. Spirakis, and B. Weihl, "Demand dispatch," *IEEE Power and Energy Magazine*, vol. 8, no. 3, pp. 20–29, May-June 2010.

[5] J. Liu, Y. Xiao, S. Li, W. Liang, and C. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications Surveys Tutorials*, vol. PP, no. 99, pp. 1–17, 2012.

[6] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Security and Privacy*, vol. 7, no. 3, pp. 75–77, 2009.

[7] NIST, *Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements*, August 2010, NISTIR 7628, available at http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf.

[8] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, June 2010.

[9] K. Moslehi and R. Kumar, "A reliability perspective of the smart grid," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 57–64, June 2010.

[10] R. Anderson and S. Fuloria, "Who controls the off switch?" in *Proceedings of the First IEEE International Conference on Smart Grid Communications, SmartGridComm10*. Maryland, USA: IEEE, October 4-6 2010.

[11] E. L. Quinn, "Privacy and the New Energy Infrastructure," February 2009, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731.

[12] A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*, ser. WPES'11. New York, NY, USA: ACM, 2011, pp. 49–60.

[13] NIST, *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*, August 2010, NISTIR 7628, available at http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

[14] Task Force Smart Grids, Expert Group 2, *Regulatory recommendations for data safety, data handling and data protection*, December 2010, available at http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf.

[15] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proceedings of the First IEEE International Conference on Smart Grid Communications, SmartGridComm10*. Maryland, USA: IEEE, October 4-6 2010.

[16] G. Kalogridis, C. Efthymiou, T. Lewis, S. Denic, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proceedings of the First IEEE International Conference on Smart Grid Communications, SmartGridComm10*. Maryland, USA: IEEE, October 4-6 2010.

[17] CEN/CENELEC/ETSI, *Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids*, May 2011, Available at http://www.etsi.org/WebSite/document/Report_CENCLCETSI_Standards_Smart\%20Grids.pdf.

[18] W. Kempton and J. Tomic, "Vehicle-to-grid power fundamentals: Calculating capacity and net revenue," *Journal of Power Sources*, vol. 144, no. 1, pp. 268–279, 2005.

[19] K. Clement-Nyns, E. Haesen, and J. Driesen, "The impact of vehicle-to-grid on the distribution grid," *Electric Power Systems Research*, vol. 81, no. 1, pp. 185–192, 2011.