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

Georgios Kalogridis, Mahesh Sooriyabandara and Zhong Fan

***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 SG components with a two-way communications network to support automated meter reading (AMR), and real-time optimisations such as load shedding/management, distributed energy storage (e.g. in Electric Vehicle, EV) and distributed energy generation (e.g. from renewable resources).

While the capabilities of communication and information technologies can allow smart communities to use energy better, the protection of the SG infrastructure is of major concern. This is because, unlike the traditional power grid, AMR is susceptible to attacks which might damage the safety and reliability of the system.

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/SG network, considering its architectural complexity, 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 careful access control.

The requirement for data privacy and data handling is of particular importance, as SM data infer information about the life of individuals. The problem of data privacy preservation is intrinsic in SM because frequent data collection from smart meters reveal a wealth of information about residential appliance usage. Data mining combined with lax controls and granular SM data collection give rise to a risk of privacy invasions.

The aim of this paper is to introduce some fundamental problems of SM security and privacy and combine known solutions into a unified security and privacy protection (USaPP) framework. We organise our material as follows. Section II discusses how USaPP contributes to previous work and the significance of this paper. Section III discusses the idea of USaPP and describes the SM system and the USaPP requirements. Section IV introduces a USaPP framework that organises SM security and privacy measures, and §V concludes this paper.

II. Relevance

A. Previous work

The scope and perspectives of existing SM/SG security and privacy framework approaches vary.

A unified key management security scheme for SG can be found in [2]. This scheme unifies existing standard security protocols, however the scope of this scheme is limited to the provision of a communications cryptosystem and does not involve the study (impact assessment) of other security components, such as physical security, access control, intrusion detection and resilience. A home Intrusion Prevention System (IPS) is proposed in [3], and its effectiveness is analysed in different attack scenarios including hacking the home network originating from the internet and cascading to a substation, and attacking the human-machine interface. Further analysis on how (distributed) attacks on load control command signals, demand side management price signals, or cloud computation load distribution algorithms might affect the load to cause malfunctions in the power system can be found in [4]. However, the above frameworks only focus on one aspect of SG protection and do not address security and privacy issues holistically.

A useful survey of SG cyber security and privacy issues is provided by Liu et al. [5]. The authors discuss threats originating from components of the system, such as devices (SMs, EVs, PLCs, RTUs, etc), networking technologies (Internet, sensor networks, etc), management systems (SCADA, Cipher Key management), anomaly detection systems, and other interwoven functionalities such as demand response. Three areas identified for further study are [5]: 1) integrity

Toshiba Research Europe Limited, Telecommunications Research Laboratory, 32 Queen Square, Bristol, BS1 4ND, UK, e-mail: {george, mahesh, zhong.fan}@toshiba-trel.com

and confidentiality of the transmitted data, 2) building a robust and efficient dispatching and management model for SCADA system, and 3) establishing a universal policy and standard for secure communication technology. While the above overview is quite comprehensive, the is an overlap between different threat categories and solutions discussed. The need to combine SG security and privacy problems and solutions and link them with distinct classes of security systems is the motivation behind this paper.

Datta Ray et al. recognise the need for a holistic approach on SG security and they propose a unified risk management system [6]. This framework considers all the interconnected vulnerabilities, different performance requirements and security priorities in the SG. However, this general methodology does not discuss particular classes of SG security and privacy issues; instead it depends on the analysis of such issues in order to evaluate the risk in different use cases.

B. *Contributions*

Providing a comprehensive security analysis of SM/SG from different stakeholders' point of view is not the objective of this paper. Instead, this study provides an overview of user-related SM problems and solutions as the basis for suggesting a unified approach. We consider the USaPP framework to be an integrated, holistic approach to the SM/SG security and privacy problems. One important design requirement for USaPP is compactness: existing security solutions correspond to distinct classes of security systems. The benefit of this framework is that is allows SM/SG security analysis and risk methodology to be developed in a structured and scalable manner.

III. Rationale and principles of USaPP SM system

A. *The idea of USaPP framework*

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 long 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 since SM is likely to be part of a critical energy infrastructure (i.e. 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 SM data and SM 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.

B. *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) [7].

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

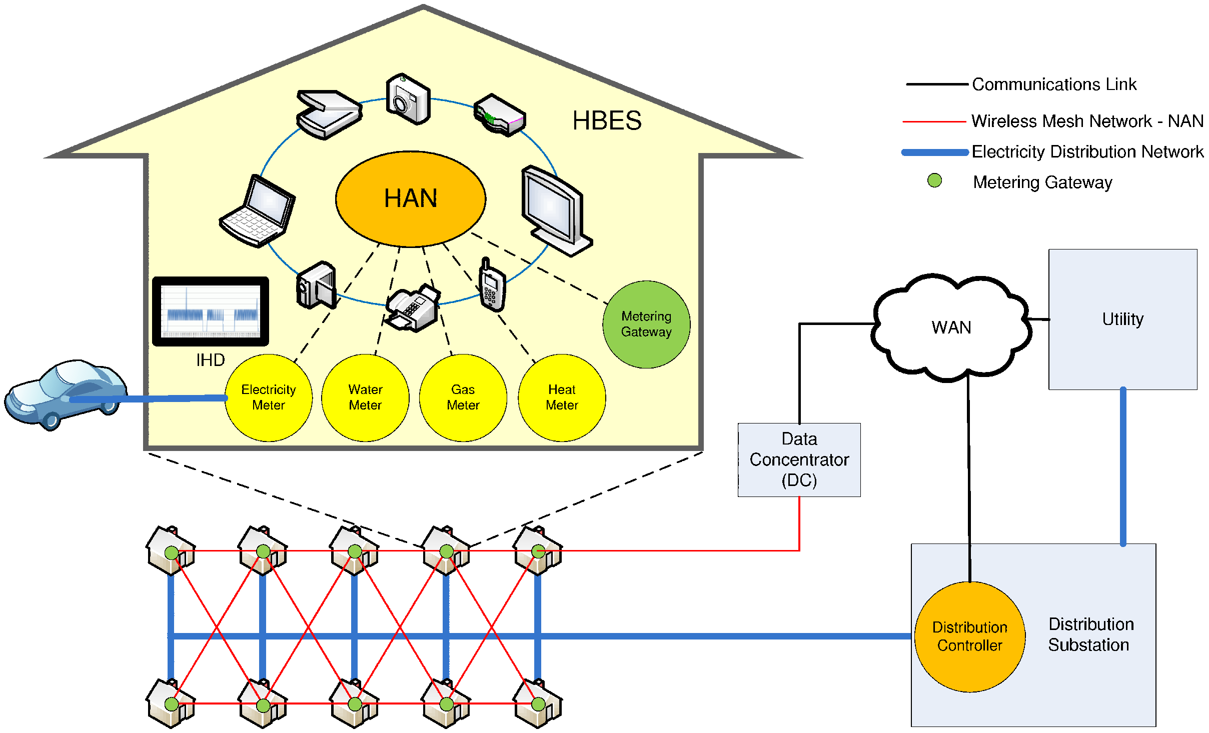


Fig. 1: Typical smart metering architecture.

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.

C. 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 [8]; 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 §III-B. 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 SM to ensure the validity of different communicating parties such as SM 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 [9]. 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.

D. 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 [10].

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.

IV. Preliminary SM USaPP framework

A. Overall architecture

Given the system requirements outlined in §III, 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.

- 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).

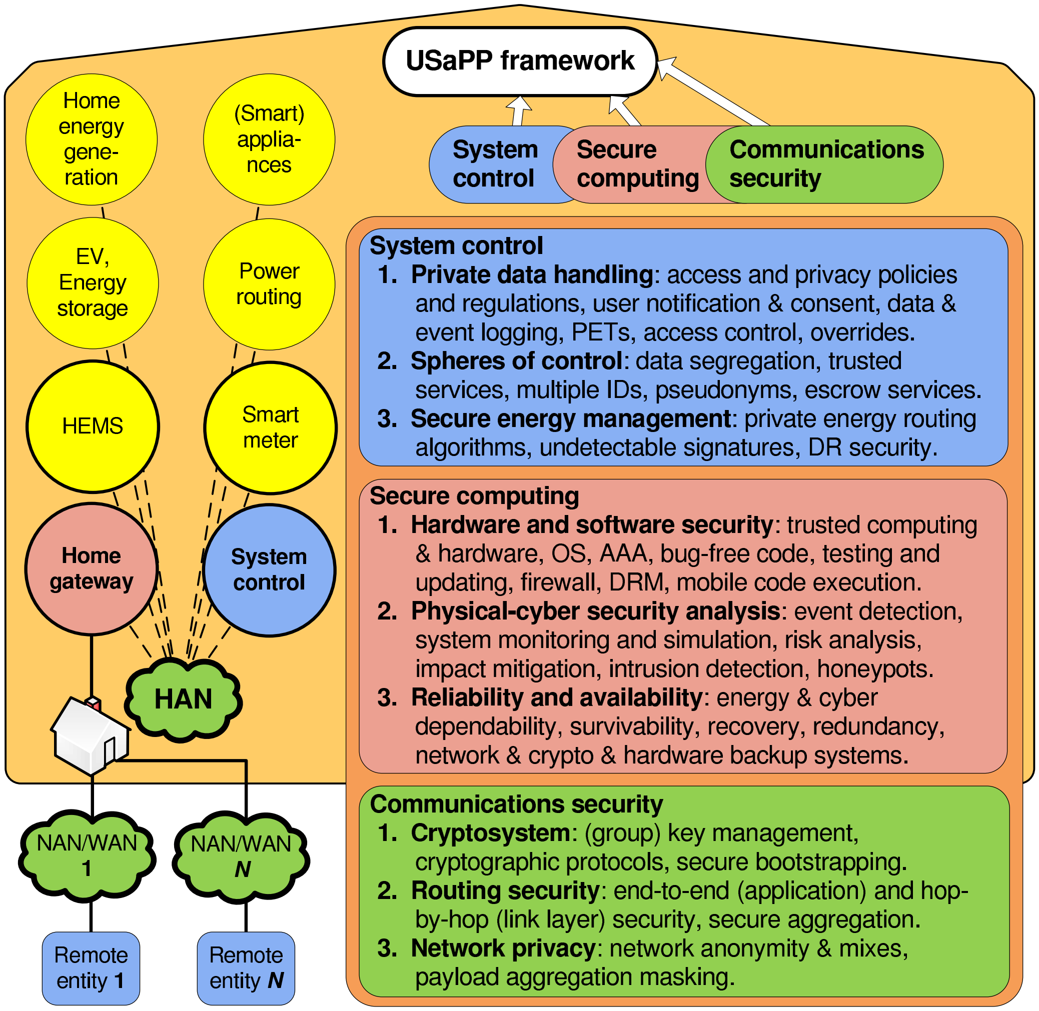
Each class integrates both security and privacy protection measures and comprises three sub-classes, which are outlined in Fig. 2 and further discussed in the remainder of this section.

B. 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 Smart Meters, 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 Smart Meters 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). IBE, in particular, is attractive as it can be deployed without prior configuration of the cryptosystem. This is because the identity (ID) of a device is used to generate unique keys. This allows easy deployment of low powered devices such as sensors because they may start sending secure messages without the need to contact a key server. In general, a mixture of hierarchical, decentralised, delegated or hybrid security schemes may be feasible. Preferably, 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, as in Fig. 3. In this case, a number of intermediate aggregators are used to optimise bandwidth usage and increase network reliability. If an end-to-end encryption scheme is employed, aggregation in intermediate wireless nodes can be as simple as concatenation of encrypted data. Alternatively, secure aggregation is feasible using additive privacy homomorphism protocols. End-to-end security ensures that data security services are resilient to compromised or rogue intermediate nodes. 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



System control

1. **Private data handling**: access and privacy policies and regulations, user notification & consent, data & event logging, PETs, access control, overrides.
2. **Spheres of control**: data segregation, trusted services, multiple IDs, pseudonyms, escrow services.
3. **Secure energy management**: private energy routing algorithms, undetectable signatures, DR security.

Secure computing

1. **Hardware and software security**: trusted computing & hardware, OS, AAA, bug-free code, testing and updating, firewall, DRM, mobile code execution.
2. **Physical-cyber security analysis**: event detection, system monitoring and simulation, risk analysis, impact mitigation, intrusion detection, honeypots.
3. **Reliability and availability**: energy & cyber dependability, survivability, recovery, redundancy, network & crypto & hardware backup systems.

Communications security

1. **Cryptosystem**: (group) key management, cryptographic protocols, secure bootstrapping.
2. **Routing security**: end-to-end (application) and hop-by-hop (link layer) security, secure aggregation.
3. **Network privacy**: network anonymity & mixes, payload aggregation masking.

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

may provide some security services such as integrity and authentication.

We note that WAN/NAN design may need to address stringent reliability requirements, such as 200 ms latency guarantees, whereas HAN may be less demanding. Both networks, however, will employ authentication and privacy control mechanisms to prevent eavesdroppers and attackers from interfering with the system.

3) Network privacy: Privacy protection requires standard security services such as confidentiality, authentication and access control. Such security services are required both when a private message needs to be communicated and processed or stored in computing systems. 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-D. In such cases, privacy can be further protected by developing *network mixes* such as *onion routing*.

The implementation of effective network anonymity services depends on the network architecture. For example consider the WSN in Fig. 3. In such network, anonymity may be accomplished if data aggregators are used as anonymisers. Similarly, 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.

Finally, we note that an SM aggregator may also offer undetectability (as defined in §III-D). 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.

C. 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).

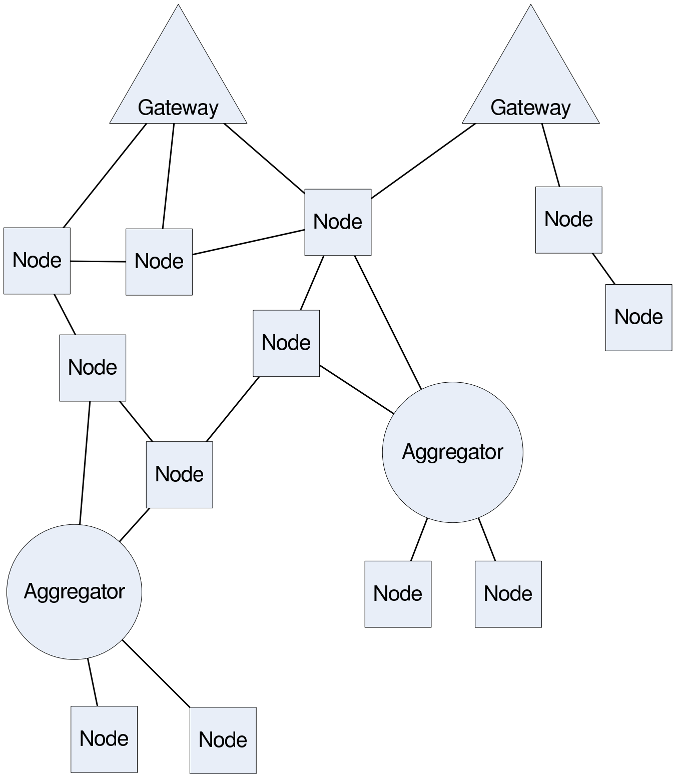


Fig. 3: Abstraction of the SM aggregation scenario.

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.

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.

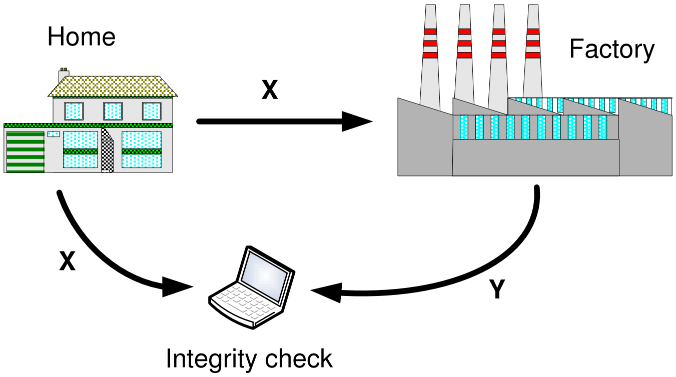


Fig. 4: Redundant measurement system to verify the integrity of the reported measurements.

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 core 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. 4 where the integrity of 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.

D. 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 [11]. 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.

Each data category could be communicated to different stakeholders as required. For example, the Expert Group 2 of the European Task Force Smart Grids [12] has recommended that technical SM data should be anonymised with means of data aggregation, as discussed in §IV-B3.

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 [13] introduces a structural difference to a smart meter within which two separate IDs are embedded, as depicted in Fig. 5: 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.

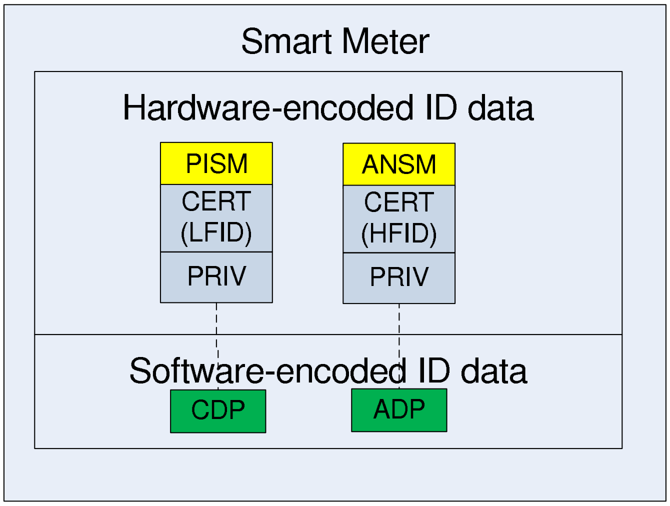


Fig. 5: Smart meter hardware architecture containing a) a Personally Identifiable SM (PISM) Profile and b) an Anonymous SM (ANSM) Profile. Each profile contains: a Certificate (CERT), corresponding hardware ID, Public Key, Private Key (PRIV), and root Certifying Authority (CA) data. The two profiles are used to create or update a Client Data Profile (CDP) and an Anonymous Data Profile (ADP).

We note that multiple-ID hardware architectures, as in Fig. 5, may support a) escrow anonymisation discussed here, b) group key management protocols for attack impact mitigation discussed in §IV-B1, or c) backup keys trust for emergency hardware control discussed in §IV-C3. This again illustrates the importance for having a USaPP design.

3) Secure energy management: The concept of privacy via undetectability discussed in §III-D 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" [11]. In this context, SM privacy can be studied as an undetectability property of appliance load signatures [14]. 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. 6. 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 §IV-D2. It is also clear that private energy management may conflict with other SM func-

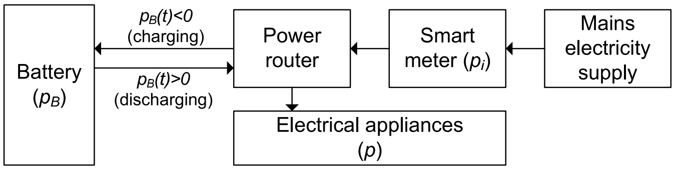


Fig. 6: The battery is discharged/recharged with power $p_B(t)$ in order to 'disguise' a given consumption load $p(t)$. The smart meter records a power trace $p_i = p - p_B - p_L$, where $p_L(t)$ is the power lost within the battery.

tionality such as DR/DSM or energy pricing arbitrage.

V. 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 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 risk analysts. 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] D. Meyer and F. Baker, *Internet Protocols for the Smart Grid*, June 2011, IETF rfc 6272.

[3] S. S. Wu, C. C. Liu, A. F. Shosha, and P. Gladyshev, "Cyber security and information protection in a smart grid environment," in *Proceedings of the 18th IWorld Congress*, vol. 18, no. 1, 2011, pp. 13 696–13 704.

[4] A. H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 667–674, December 2011.

[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, December 2011.

[6] P. Datta Ray, R. Harnoor, and M. Hentea, "Smart power grid security: A unified risk management approach," in *Proceedings of the 2010 IEEE International Carnahan Conference on Security Technology (ICCST)*, October 2010, pp. 276–285.

[7] ETSI, *Machine-to-Machine communications (M2M); Smart Metering Use Cases*, May 2010, TR 102 691, v1.1.1.

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.