2012 IEEE 36th International Conference on Computer Software and Applications Workshops

Attack Vectors to Metering Data in Smart Grids under Security Constraints

Florian Skopik, Zhendong Ma
Safety and Security Department
AIT Austrian Institute of Technology
{florian.skopik|zhendong.ma}@ait.ac.at

***Abstract*—The electric power grid is facing a major paradigm shift, away from static structures to a more intelligent and flexible energy utility. In order to increase the efficiency of the power grid and implement novel services, such as dynamic pricing, rigorous and fine-grained monitoring of the grid status is required. However, this approach generates huge amounts of sensitive metering data, and requires sharing with various parties to be finally effective. In this regard, strong security measures must be integrated in the design of deployed infrastructures from the beginning in order to facilitate customer trust in this novel technology. Hence, this paper presents the most important results of an in-depth analysis of threats and attack vectors that could impede the wide adoption of automatic metering in smart grids. These results are valuable input for future architectures and designs of critical system components incorporating effective security and privacy protection mechanisms.**

***Keywords*-smart grid security, metering data infrastructure**

I. Introduction

The electric power grid is by far the most important technical infrastructure used today and the basis for modern life. It is essential for all current networked services, such as telephone, television, or the Internet. With the emergence of electric cars, the power grid will also ensure our mobility and thus increase its role even more. Reliable, dependable and secure energy supply is thus of paramount importance not only for the industry, but for the whole society. Changing requirements on the power grid in terms of supply capacity, load conditions, and adaptability lead to an ongoing modernization and a major shift from a static public power grid to a more flexible one that can cope with today's challenges. The *Smart Grid* initiative aims at advancing the traditional power grid to an intelligent utility [1], [2]. As defined in [3], *a smart grid is an electricity network that can cost-efficiently integrate the behavior and actions of all users connected to it - generators, consumers, and those that are both - to ensure an economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety.*

The smart grid promises numerous advantages compared to today's grid technology. Among the most significant ones are massive cost reduction through automatic meter reading, dynamic pricing allowing the customer to switch between various energy providers in short time intervals, better monitoring of the grid's health and thus applying faster countermeasures to impending black outs, and allowing the feedback of excessive energy produced by customers (e.g., by private wind turbines or solar panels). By effectively transforming today's public power grid to a smart grid, novel system features are introduced, including two-way communication services for meter reading, automatic accounting and billing, and remote control of devices. But the vision of the future smart grid goes even further. In the near future, novel community portals will enable customers to compare energy consumption data with other households, set up social campaigns in order to strengthen energy awareness, and dynamically feed back self-generated green energy from own solar panels and wind turbines.

A key factor to achieve these ambitious goals is the comprehensive roll-out of smart meters and the construction of a reliable smart metering infrastructure. Comprehensive and advanced security and privacy mechanisms are needed not only to guarantee smooth and reliable operation and to cope with today's security challenges, but also to gain customers' trust in this new technology. An identification of threats and structural analysis of vulnerabilities is an important step toward securing smart grid infrastructures and the basis for developing advanced security and privacy protection mechanisms.

The massive amounts of data continuously produced (meter readings, status messages etc.) need to be shared by various grid stakeholders to deliver efficient services:

- *Grid Operators* need real-time metering data to ensure the smooth operation of the network (e.g., detect and compensate local overloads).
- *Energy Providers* use aggregated data to estimate mid-term energy requirements of customers.
- *Billing Companies* demand for accurate consumption data to implement envisioned flexible price models.
- *Third-party Value Added Services* are used to generate consumption profiles and potentially compare them within so-called 'energy saving communities'.
- *Governmental Agencies* might demand access in preparation of lawsuits.

Complex security and privacy concepts are already in place to guarantee smooth operation of the smart grid and

978-0-7695-4758-9/12 $26.00 © 2012 IEEE
DOI 10.1109/COMPSACW.2012.34

protect customers from fraudulent individuals, and even more advanced mechanisms need to be developed to cope with today's security challenges. Therefore, in this paper we provide a structured analysis on vulnerabilities and threats related to smart grids. Because the smart metering infrastructure is envisioned to be a rather open system to allow access from various devices and users, our focus is on the issues related to smart metering infrastructure. Our main contributions are twofold:

- *Smart Grid Security Principles.* We highlight a typical smart grid structure, show potential attack targets in the whole system, and outline attack incentives, and methods.
- *Analysis of Threats.* We outline actual threats and potential weaknesses in today's smart meters and utilized network technologies. Here, we report only the highlights of an in-depth survey.

The remainder of the paper is organized as follows. Background and related work is discussed in Section II. Section III outlines a basic smart metering infrastructure and key principles of information security. Section IV deals with threat analysis fundamentals and highlights the results of an in-depth survey. Finally, Section V concludes the paper.

II. Background and Related Work

Smart Grid technologies have received major attention in both academia and industry in recent years. Various works discuss the basics of the smart grid, such as its structure, application, and potential impact [1], [2]. Others cover established and recently developed technical standards [4]. The European Union plans to replace traditional electricity meters with smart meters until 2020 to a large extent, which basically motivates us to take a detailed look at privacy and security threats of this technology [3].

The electric grid is perhaps the most critical infrastructures today, and thus, safety, i.e., reliability and availability is a top priority. Many works investigate how smart meters and related technologies can contribute to an even more reliable grid, e.g., by applying novel self-healing mechanisms [5]. Moreover, in the last months – after starting considerable roll outs of this technology – security and privacy issues have become the focus of many discussions [6]. Particular research deals with effective key distribution [7] and management for devices with very limited computational power [8] to enable efficient encryption of meter readings and access control (similar to Pay-TV access control systems [7]). A key success factor of many smart grid features is the extensive monitoring and logging of consumption data. The prediction of required electric energy is important to avoid overloads and blackouts in the system. However, by observing the consumers' electricity consumption behavior, major privacy issues arise [9]. Therefore, considerable research has been conducted, addressing these inherent problems, e.g., by anonymization of metering data [10] or applying privacy-by-design patterns [11]. From the industrial side, efforts have been made to set up security guidelines and best practices, e.g., by the Advanced Meter Infrastructure (AMI) security task force[1]. Due to the fact that the electric power grid is a strategic target in case of wars, investigations on the reliability and resilience of smart grids [12] are necessary, and essential to devise security architectures against cyber attacks [13]. Furthermore, novel security mechanisms [14] require sophisticated threat models in order to verify and validate their implementation.

The smart grid will be much more tightly connected to the Internet than often expected. Different works deal with connecting the smart grid to the Internet through Web services [15], and enable agent-based approaches for energy distribution [16]. Web-based applications and platforms[2,3,4] let people manage their consumption behavior online. For instance, comparing energy demand with people having similar demographic background might discover unanticipated energy saving opportunities. Energy saving campaigns and competitions have great potential to increase the awareness for energy and its wealth. Since reliable and safe control and operation of smart grid depends on the information from smart metering infrastructures, in our paper, we focus on information security in the metering infrastructure.

III. Smart Grid Security Principles

A. Entities in Smart Metering Infrastructures

We divide our analysis on security threats in the smart metering infrastructures according to the hierarchical structure illustrated in Figure 1. Here, major entities and their connecting networks are separated in a layered model:

- *Intelligent Electric Appliances:* are connected through a local home area network (HAN) to the smart meter in order to report detailed energy consumption data, but also to be controlled by the smart meter and utility company respectively based on dynamic price models.
- *Smart Meters:* measure the total power consumption and (optionally) collect the consumption of single devices. Data is reported to the next concentrator node through a neighborhood area network (NAN).
- *Concentrator Nodes:* monitor and collect data from several smart meters in proximity. More intelligent devices can preprocess and compress this data which is pushed to one or several data centers via a high-speed backhaul (WAN).
- *Utility Data Centers:* stores and processes received data used for accounting and billing (even by third parties), but also for monitoring and actively controlling the power grid status.

[1] AMI-SEC: http://osgug.ucaiug.org/utilisec/amisec
[2] OPower Company: http://opower.com
[3] Smart Energy Group: http://www.smartenergygroups.com
[4] Energy Lens: http://www.energylens.com

- *Social Networking Platforms:* People may allow value-added applications to access online data about their energy consumption. This enables them to compare meter readings, exchange excessive energy, and set up social campaigns for energy awareness.

In this paper, we structure the analysis on threats and vulnerabilities in three tiers as highlighted in Figure 1:

- *Tier 1:* deals with threats to electric appliances, smart meters and their uplink to concentrator nodes. This part is often referred to as the 'last mile' and is considered as most vulnerable to attacks.
- *Tier 2:* deals with vulnerabilities of the uplink from smart meters over concentrator nodes to data centers and interfaces to Web-based applications.
- *Tier 3:* deals with Web-based applications and community networks that use gathered meter data.

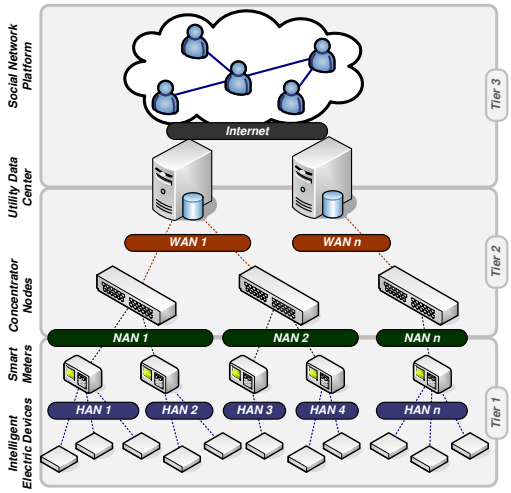

Figure 1. Structure and entities in smart metering infrastructures.

B. Key Principles of Information Security

Security-sensitive topics [17] are typically discussed in context of the so called CIA triangle (see Figure 2), highlighting major aspects with respect to three pillars: *confidentiality*, *integrity*, and *availability*. Metering services are essential to ensure reliable energy provisioning, and meter readings are highly sensitive data whose protection is a major objective in future infrastructures. Therefore, we follow the same approach, and further outline fundamental areas of smart meter infrastructures with respect to these three pillars.

Confidentiality is concerned when it comes to creating, transferring, processing, and storing customer data, either dynamically produced data, such as meter readings and energy consumption profiles, or static data, including credit card information used by the energy provider to account for services. In today's information society, customer data is an highly important asset for every company, and the exploitation of user profiles has to be avoided by appropriate privacy preserving mechanisms.

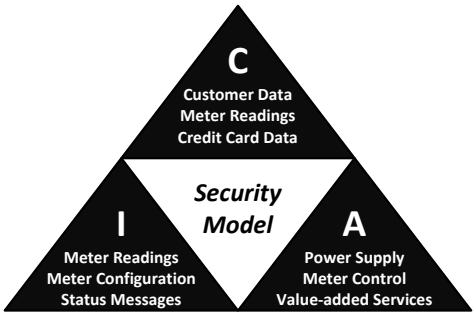

Figure 2. Confidentiality-Integrity-Availability objectives.

Integrity of reported energy consumption data is of paramount importance since this information is used for accounting and billing. Numerous possible frauds need to be prevented, such as a customer sends tampered meter data in order to pay less; or make someone else to pay more. Thus, manipulation of the smart meter itself or injection of tampered messages in the network must be avoided (or at least detected and compensated). Furthermore, injecting wrong status messages in the communication network might cause problems in the net management, e.g., reporting overload messages might urge the utility company to reshape the power grid's structure.

In order to facilitate trust between all stakeholders, i.e., customers and electricity providers, and utility company, accounting and billing processes need to be as transparent as possible. For instance, customers should have the possibility to visualize the current energy consumption level, either online or on a home display.

Availability concerns are twofold: From a customer's perspective the availability of electricity is most vital; meaning, no one is able to turn off electricity accidentally or maliciously. From a utility company's perspective remote meter readings are essential to prevent energy theft and keep the business running. Furthermore, status messages delivered from smart meters can be used to actively reconfigure the grid in case of (temporally) unexpected load conditions. Thus, the availability of the smart meter communication is essential here.

C. Smart Grid Protection Objectives

We identified the following objectives to be the most important ones to be protected in the future smart grid: (i) *Availability of the Power Grid.* This includes correct operation of energy generation, transmission, and distribution as in today's grid. However, besides physical attacks, numerous cyber-attacks are possible to interrupt correct operation, such as tampered control messages which may cause overloads or temporal blackouts. (ii) *Legitimate Power Consumption and Delivery.* The goals are, on the one side to prevent

energy theft and ensure consistent measurement of obtained energy; on the other side the correct measurement of fed back energy in case of the integration of private solar panels and wind turbines. Transparent billing an accounting are evident to establish and maintain trust relations between consumers and producers. (iii) *Privacy of Consumers.* Secure power consumption data handling (including, transmission and storage) is of paramount importance, as well as privacy-aware profiling and mining of behavior patterns. The goal is to avoid the exploitation of real-time energy consumption monitoring mechanisms.

IV. Structured Threat Analysis

Before we can rate the risks of potential attacks, we discuss the basic incentives of attackers, their targets, and fundamental methods.

A. Attack Incentives

An attacker can be motivated by various reasons to manipulate and attack the smart grid. Similar to most other infrastructure services, we identified the following incentives as the most considerable ones: (i) *Financial Gain.* This includes for instance simple energy theft by manipulating the own smart meter. Burglars might aim at obtaining consumption behavior patterns by eavesdropping meter readings to find out when someone is not at home. Hackers might further act on behalf of others due to economic reasons, e.g., harming competitors with targeted black outs. (ii) *Personal Revenge.* An attacker might black out particular households or companies due to personal reasons. A more sophisticated attack can involve the transmission of tampered meter data so that a victim is billed an extraordinary high amount of energy. (iii) *Looking for Hacker Community Acceptance or Chaos.* Here an attacker wants to prove his own capabilities, e.g., by provoking wide-spread power outages. Besides that, political reasons can also be a motivation, such as coordinated attacks on fur factories by radical animal rights activists.

B. General Threats

In a complex system of systems, such as the future smart grid, high interconnectedness of components provide virtually uncountable opportunities for attackers. In particular, the normal smart grid's mode of operation can be disturbed or even interrupted on various layers (as discussed in [18]) of the whole system.

System-level threats refer to risks regarding the regular operation of the grid. Most commonly discussed threats include, (i) *HAN subversion or takeover*, where near field networks are targeted; (ii) *network intrusion by strangers*, typically aims at IP-based NANs; (ii) *denial of service* is achieved if the delivery of electricity is interrupted; (iv) *credential compromise* exploits holes in authentication mechanisms to insert untrusted system components (e.g., tampered meters); (v) *backend compromise* enables an attacker full access to the grid management services.

Threats to theft of service are (i) *meter substitution*, where an installed meter is replaced by a tampered one reporting lower consumption than the actual one; (ii) *meter swapping*, where one can swap the meter between a location with high energy usage and a location with low energy usage; (iii) *meter interface manipulation* so that the meter reports no or wrong usage data.

Threats to privacy and confidentiality are (i) *message interception* in HANs and NANs, based on the technology (wired or wireless) in place; (ii) *forwarding point compromise* enables an infected concentrator node (or gateway) to forward data to unintended recipients; (iii) *backhaul IP network interception* concerns the IT network infrastructure in the large scale.

Notice, further orthogonal threats, such as social engineering to obtain credentials or cryptographic keys, are not discussed in depth here.

C. Tier 1 Threats: Smart Meter Attack Vectors

The HAN is currently used by intelligent electric devices to report their energy consumption and status to the meter[5]. Sniffing this traffic threatens data confidentiality (and thus privacy of the concerned customer); and can furthermore be used to discover cryptographic keys. With (symmetric) keys one can send tampered messages to the meter, threatening the integrity of meter readings and availability of the whole service (if sending wrong status messages). If a smart meter is shielded from its NAN, meter readings are not available to the utility company. Moreover, as a security measure, the smart meter firmware might be designed to switch off power supply in that case. Manipulating a smart meter, either hardware through swapping components or software, to report false readings, concerns the integrity of the consumption profile at the utility backend. Accidental or

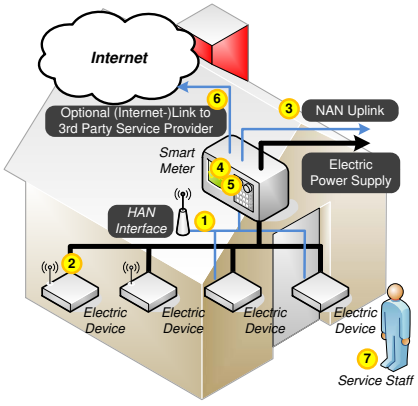

Figure 3. Potential attack actions around the smart meter.

[5]Notice, we do not consider the opposite direction, enabling a meter to control appliances.

Table I
SMART METER ATTACK VECTOR SUMMARY.

#	attack action	estim. effort	c	i	a
1	HAN sniffing	low – medium	x		
2	HAN message tampering	medium – high		x	x
3	sm. meter NAN shielding	low			x
4	sm. meter false reporting	high		x	
5	sm. meter swapping	low		x	
6	configuration manip.	medium	x		x
7	social engineering	n/a	x	(x)	x

Table II
UTILITY ATTACK VECTOR SUMMARY.

#	attack action	estim. effort	c	i	a
1	NAN sniffing	medium – high	x		
2	NAN comm. blocking	medium			x
3	NAN msg. tampering	high		x	x
4	neighbor meter DoS	high			x
5	concentr. node DoS	medium			x
6	utility data center intr.	very high	(x)	(x)	(x)

malicious manipulation of the meter configuration can cause the meter to report to a wrong service endpoint; especially if third party services, e.g., for data aggregation and profiling[6,7], are used. Finally, the application of social engineering on service personnel can greatly harm confidentiality (and maybe integrity) of data, as well as availability of services. A summary is shown in Figure 3 and Table I.

D. Tier 2 Threats: Electric Utility Attack Vectors

The purpose of the NAN is twofold; first, the smart meter pushes monitoring data to concentrator nodes (or might even exchange data with another smart meter), second, the utility backend (or concentrator node) sends control messages to smart meters, e.g., black out a customer who is unwilling to pay. Since the NAN reaches every single household, there is a high probability of sniffing attempts. Depending on the physical structure of the communication network a malicious attacker (see the red house in Figure 4) can eavesdrop data from nearby NAN nodes. This action threatens the confidentiality of data if not properly encrypted. Furthermore, since numerous smart meters are sharing the same media, message blocking by manipulating the communication media is a threat to the availability of neighbors' smart grid services. Message tampering harms the integrity of data (e.g., when fabricating false readings), and threatens the availability of services when dealing with fake status messages. Moreover, even the availability of a nearby smart meter can be threatened by an attacker, by the means of message tampering. A denial-of-service (DoS) of the concentrator node could potentially be achieved through distributed attacks, in particular by flooding the NAN with fabricated status messages and false readings in very short time intervals. In theory one could even pass a concentrator node and gain access to the backend data center. However, potential attacks highly depend on the smart grid system properties, for example, what parts of the backend could be reached and harmed. Overall, notice, that the required effort and success rate of attacks on the NAN highly depends on the network topology as well as employed protocols (for instance, IP-based) and technologies (for instance, public key infrastructure v.s. symmetric encryption with static keys). Today, we lack experience regarding the application of standardized technologies for NANs, thus, Table II summarizes estimated results under realistic assumptions only.

E. Tier 3 Threats: Web Services Attack Vectors

WAN sniffing compromises the confidentiality of meter readings. Denial of service attacks can either be performed over the smart metering network (referred to as WAN), or the Internet; depending on the attack channel. In many infrastructures the metering infrastructure WAN can be realized through virtual connections over the Internet. In summary, either the backend service that receives the metering data is

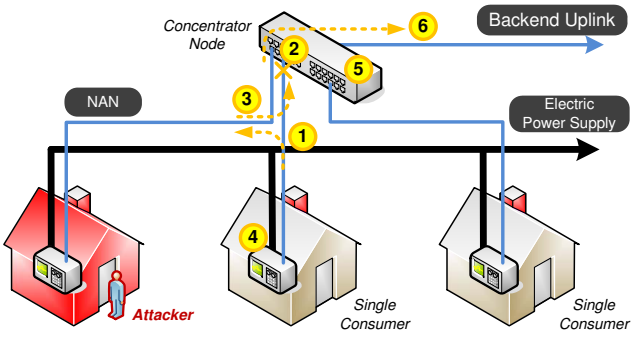

Figure 4. Potential attack actions against the NAN and utility.

[6]OPower Company: http://opower.com
[7]Energy Lens: http://www.energylens.com

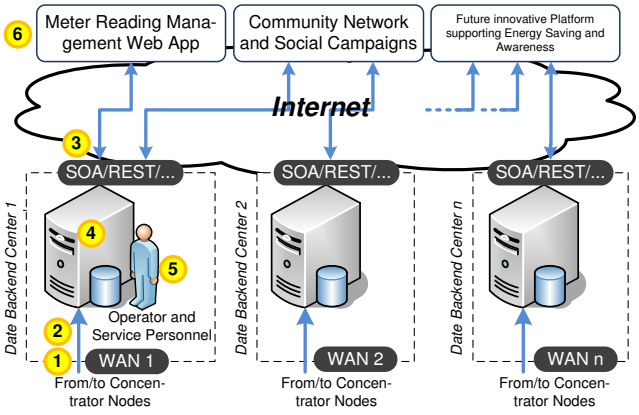

Figure 5. Potential attack actions against the backend center and (potentially third party) Web applications.

attacked or the Web application frontend. In case an intruder gets access to the backend, s/he could potentially change or delete data, thus threatening the integrity of stored meter readings. However, further assessment would require the investigation of a concrete backend instance and thorough analysis of its design. A common threat in an infrastructure involving service personnel is social engineering in order to gain unauthorized access to aggregated meter readings and user profiles. Table III summarizes potential security risks. The final entry in Table III, deals with attacks against Web Apps, which can either be technical attacks against standard software with known vulnerabilities, attacks on the accessing network (e.g., WiFi sniffing) or social attacks, including shoulder surfing. Based on the actual attack all three aspects of CIA are threatened.

Table III
ONLINE PLATFORM ATTACK VECTOR SUMMARY.

#	attack action	estim. effort	c	i	a
1	WAN sniffing	n/a	x		
2	data backend DDoS (WAN)	n/a			x
3	data backend DDos (Internet)	n/a			x
4	data backend intrusion	n/a	x	x	x
5	data theft through social eng.	n/a	x		
6	attacks against Web Apps	low-medium	x	x	x

V. CONCLUSION AND FUTURE WORK

We like to conclude the analysis of threats and technical vulnerabilities in future smart metering infrastructures with a set of recommendations for risk mitigation. Derived from the analysis' findings, the design of future smart grid infrastructures need to be centered around:

- Physical robustness and tamper resilience of smart meters and concentrator nodes in order to hinder numerous hardware hacks and attacks.
- Authentication of users and devices using strong passwords, digital certificates and signatures.
- Authorization of users and devices to grant them least privileges to access resources and services.
- Encryption of communication data and user data in the utility data center.
- Integrity and plausibility checks of data, such as meter readings, grid status messages, and network traffic.
- Training of technicians and service staff to prevent social engineering.

All measures of this list are required in order to ensure security and privacy of smart grid stakeholders. Work reported in this paper is only the first – but an essential – step toward a secure smart metering infrastructure. The expected amount of dynamically produced data raises novel research challenges regarding security of all smart grid stakeholders as well as privacy of customers.

Future work mainly deals with further technical in depth analysis of today's threats to the smart grid infrastructure. Further future work includes the design and implementation of a layered architecture covering the various security aspects and coping with threats on the physical layer (device accessibility, network infrastructure), logical layer (software, communication protocols), and administrative layer (employee background checks, training on repelling social engineering).

REFERENCES

[1] Massoud and B. F. Wollenberg, "Toward a smart grid: power delivery for the 21st century," *IEEE Power and Energy Magazine*, vol. 3, no. 5, pp. 34–41, Sep. 2005.

[2] L. H. Tsoukalas and R. Gao, "From smart grids to an energy internet: Assumptions, architectures and requirements," in *DRPT*, 2008, pp. 94–98.

[3] European Regulators Group for Electricity and Gas (ERGEG), "Ergeg-public consultation: Position paper on smart grids no. e09-eqs-30-04," Berlin, 2010.

[4] R. DeBlasio and C. Tom, "Standards for the smart grid," in *IEEE Energy 2030 Conference*, 2008, pp. 1–7.

[5] M. Amin, "Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid," *PES General Meeting*, pp. 1–5, 2008.

[6] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues." *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[7] S.-Y. Wang and C.-S. Laih, "Efficient key distribution for access control in pay-tv systems." *IEEE Transactions on Multimedia*, vol. 10, no. 3, pp. 480–492, 2008.

[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, 2010.

[9] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy Magazine*, vol. 7, no. 3, pp. 75–77, 2009.

[10] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," *Distribution*, pp. 238–243, 2010.

[11] A. Cavoukian, J. Polonetsky, and C. Wolf, "SmartPrivacy for the smart grid: embedding privacy into the design of electricity conservation," *Identity in the Information Society*, vol. 3, no. 2, pp. 275–294, Aug. 2010.

[12] K. Moslehi and R. Kumar, "A reliability perspective of the smart grid," *2010 Innovative Smart Grid Technologies ISGT*, vol. 1, no. 1, pp. 57–64, 2010.

[13] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in *Innovative Smart Grid Tech.*, Jan. 2010, pp. 1–7.

[14] A. P. A. Ling and M. Masao, "Selection of model in developing information security criteria for smart grid security system," *CoRR*, vol. abs/1109.2697, 2011.

[15] C. Warmer *et al.*, "Web services for integration of smart houses in the smart grid," in *Grid-Interop - The road to an interoperable grid, Denver, Colorado, USA*, November 2009.

[16] M. Pipattanasomporn, H. Feroze, and S. Rahman, "Multi-agent systems in a distributed smart grid: Design and implementation," in *Power Syst Conf and Exp*, 2009, pp. 1–8.

[17] R. J. Anderson, *Security engineering - a guide to building dependable distributed systems*, 2nd ed. Wiley, 2008.

[18] SilverSpring Networks, "Whitepaper: Smart grid security: Myths vs. reality," 2011.