Adaptive Security and Privacy in Smart Grids: A Software Engineering Vision

Mazeiar Salehie[1], Liliana Pasquale[1], Inah Omoronyia[1], and Bashar Nuseibeh[1, 2]
[1] *Lero – The Irish Software Engineering Research Centre, University of Limerick, Ireland*
{mazeiar.salehie, liliana.pasquale, inah.omoronyia, bashar.nuseibeh}@lero.ie
[2] *Department of Computing, The Open University, Milton Keynes, UK*

***Abstract*— Despite the benefits offered by smart grids, energy producers, distributors and consumers are increasingly concerned about possible security and privacy threats. These threats typically manifest themselves at runtime as new usage scenarios arise and vulnerabilities are discovered. Adaptive security and privacy promise to address these threats by increasing awareness and automating prevention, detection and recovery from security and privacy requirements' failures at runtime by re-configuring system controls and perhaps even changing requirements. This paper discusses the need for adaptive security and privacy in smart grids by presenting some motivating scenarios. We then outline some research issues that arise in engineering adaptive security. We particularly scrutinize published reports by NIST on smart grid security and privacy as the basis for our discussions.**

***Keywords*- Smart grid; Adaptive software; Security and privacy; Security requirements;**

I. INTRODUCTION

The smart grid promises sustainability, reliability and higher awareness of energy generation, distribution and consumption, by managing the electricity grid with information technology. However, rich features and interfaces of smart grid can introduce vulnerabilities and increase security and privacy risks. For example, deploying a weak authentication method by a customer may lead to unauthorized remote access to his/her meter data. Although security and privacy concerns in electricity grids are not new (illustrated by $6 billion in losses due to fraud in the US alone in 2009 [1]), the smart grid extends the attack surface through its augmented interfaces and improved flexibility of access to services and information.

Although security and privacy requirements at "design time" have been discussed extensively since the early initiatives of smart grids, these requirements may be incomplete, may fail or might no longer be satisfied by a system during its operation (at "run time"). This may be the result of changing critical assets in the grid (such as energy-related information or appliances), emerging threats, or varying environmental conditions. Moreover, architecture and design decisions as well as deployed technologies |(such as adopting cloud computing architectures), could have security and privacy implications for the smart grid. Such implications may only be observed during operation or as consequences of failures in the grid (e.g., blackouts). All these cases need to be detected and managed at run time efficiently and effectively.

Adaptive software models and technologies promising to address some of these issues by handling uncertainty and automating monitoring, analysis, decision-making, and the application of security controls. Indeed, security controls can be adapted to protect critical assets continuously across all the seven domains of the smart grid identified by NIST [2]: transmission, distribution, bulk generation, operations, service provider, markets and customer domains.

In the rest of this paper, first we review security and privacy concerns in smart grids. Then we investigate demands for adaptive security and privacy in this domain. Finally, we outline software engineering research issues in realizing adaptation in smart grids.

II. SECURITY AND PRIVACY IN SMART GRIDS

This section briefly reviews security and privacy issues in the smart grid, particularly using NIST reports.

A. Security

Protecting valuable assets within a system boundary is the ultimate goal of security. In a smart grid, energy is a primary critical asset that needs be protected across a very wide and often changing system boundary. However, related data, such as meter data, audit trails, billing and pricing data, customer information, financial and marketing data, can also be as valuable as energy. Furthermore, equipment and services for metering, energy distribution, transmission, load management and information transmission and processing also need to be protected. To this end, some well-known security goals need to be achieved and maintained for these assets [3]:

- *Confidentiality* of electricity market data, corporate information, customer information, and meter data;
- *Availability* to deliver in-range time latency for control signals, meter reading, power quality information, incident response plus availability of power-enabled devices belonged to customers;
- *Integrity* to ensure source of data is authenticated, timestamp is known, quality of data is known, and data or control commands are not intercepted;
- *Accountability* to ensure who is responsible for commands in the grid, and all signals and events are audited in a proper way

Possible threat agents for these goals in almost all seven domains include [3]: foreign countries, some employees, hackers, and industrial competitors, to name a few. Threat motivations include energy theft, sabotage, revenge, monetary gain, and mistakes.

Depending on the adopted architecture, technology, and the awareness of human agents, different vulnerabilities may be introduced to the system. For instance, to lower costs, the computational ability of meters may be limited. This can lead to using weaker security controls such as weaker encryption algorithms. Outdated firmware, slow network connections, insecure remote configurations or patch updating are few other possible vulnerabilities. These vulnerabilities can be exploited in a variety of ways. For example, Carpenter et al. [4] describe possible attacks for Advanced Metering Infrastructure (AMI), including power and clock glitching, fuzzing, and malicious framework patching.

One of the current trends in smart grid is the use of cloud architectures. For example, IBM and C&W are developing a UK national smart energy cloud. Verizon and AT&T are also working on cloud-based smart grid[1], which leverages the combination of mobile and cloud computing. Multi-tenancy, storing data in several jurisdictions, and cross-organizational data access in cloud environments could increase risk of protecting critical assets. On the mobile side, vulnerabilities of firmware and applications may also be problematic.

B. Privacy

Smart grids collect, transmit and store vast amounts of privacy-sensitive data about people, which can be extremely attractive to other people and businesses. NIST has considered four aspects of privacy: personal information, personal privacy, behavioral privacy, and personal communication [3]. Personal data available in the smart grid includes: name, address, banking information, meter data, bill, in-house energy generation, and energy and service provider(s) [3]. Moreover, other information can be inferred from this data. For instance, life styles and usage patterns can be extracted from meter data using data mining techniques.

NIST points out that information may be exploited by different agents for a variety of purposes in smart grids [3]:

- Insurance companies: determining health care premiums based on customers' life styles
- Marketers: advertising based on usage patterns
- Police and law enforcers: identifying illegal or suspicious behavior (e.g., planting marijuana)
- Landlords: verifying lease compliance
- Criminals: Remote surveillance
- Fraudsters: Attributing energy consumption to others

Privacy requirements are needed to protect privacy-sensitive information in order to mitigate risks of misuse by the above agents.

III. DEMAND FOR ADAPTIVE SECURITY AND PRIVACY

This section discusses triggers for adaptive security and privacy in smart grids through some motivational scenarios.

A. Adaptive Security

Security requirements are describe the need to protect assets in a system boundary. As noted by Shorter and Hollenbaugh [9], asset protection is key activity in automating security management for smart grids. However assets in the smart grid boundary may change. Possible changes include adding, removing, or changing criticality (i.e., value) of assets due to contextual factors. Consider the following scenario related to changing assets:

Scenario A *– A new organization is established in a building. Valuable devices are moved into the building and critical information is collected, stored and processed in the organization.*

In this scenario, security of energy, related equipment, and information are all changing for this building, and need to be examined. Asset changes increase security risks, which in turn might render security controls ineffective or might change the priorities of security requirements. Devices (such as electrical appliances) may be sabotaged remotely, shut down, or be manipulated with malicious intent. Power-enabled security controls can be also be compromised to access information and sensitive devices.

Other than assets, contextual changes (e.g., economic), newly discovered vulnerabilities (e.g., bugs in the system), and failures of security controls may lead to similar situations. In such cases, proactive adaptation can reconfigure security controls to mitigate high risks. In Scenario A, critical devices can be protected by stronger access control to energy sources and management systems.

On the other hand, reactive actions may be required to respond to incidents and detected abnormalities. For example assume the following scenario:

Scenario B *– Actual electricity usage in an area does not match with the reported meter data. This might be a sign of energy theft, although leakage in the distribution network or malfunctioning transformers could cause the same problem.*

In this scenario, adaptive security will check integrity of data and audit trails to investigate root causes of the problem. Auditing levels can be adjusted and stronger counter-measures applied temporarily to prevent possible fraud. Salehie et al. [5] analyzed AMI security requirements and discussed some possible security cases. For example, if the audit trail frequently overflows, it might be a sign of tampering with the meter or altering metering data.

The way customers and organizations in the smart grid access data and services is also important in security and should be considered during adaptation. Access to the grid's critical data and services through browsers or mobile apps, via insecure devices and data networks, may need adjustment to security controls at runtime.

B. Adaptive Privacy

NIST recommends that privacy use cases should be developed to track information flow inside the smart grid to identify and mitigate privacy threats [3]. However, during the system operation private information might be revealed or inferred by unauthorized parties, similar to incidents in mobile phones. Adaptive privacy aims to monitor information transmission actively in the grid to detect and mitigate possible threats.

1 http://gigaom.com/cleantech/verizon-brings-the-smart-grid-to-the-cloud/

One of triggers for adaptive privacy is contextual change, such as changes in spatiotemporal factors. Consider the following scenario for this case:

Scenario C – *A VIP or celebrity is moving to a house permanently or temporarily. Different parties may find this person's private information beneficial, for example: press and marketing agencies.*

In this scenario, privacy policies need to be adjusted to control transmissions of energy-related information in this new building. In many situations, mobility can introduce these contextual changes and privacy concerns. Consider the following scenario:

Scenario D *– A person charges his electrical car en route when he is travelling. The fee is applied to his electricity bill, which means the companies owning the power stations report the expenses to the utility company with whom this person has a contract.*

In this scenario, a person's location, trip plans, and long-term behavior can be revealed to several companies. This person may want to know who knows what about him, and be notified if any of these companies share this information with other businesses (e.g., car insurance agencies). To deal with these scenarios, adaptive privacy needs to monitor information transmission, detect possible privacy threats, and mitigate them.

IV. Engineering Adaptive Security and Privacy

This section outlines software engineering research issues in realizing adaptive security and privacy in smart grids. We use the terminology used by Salehie and Tahvildari [8], in which an Adaptation Manager (AM) is defined as the external embodiment of the adaptation loop.

A. Monitoring and Analysis

The AM needs to monitor and analyze changes in the grid and its environment at runtime. NIST defines continuous monitoring requirements [3] (e.g., SG.CA-6) that are useful for this purpose, although the human role is central in fulfilling them. A major challenge in monitoring and analysis is uncertainty due to imprecision and limited knowledge. Uncertainty is particularly relevant in the security domain, for example, for measuring risk. Therefore, the AM would probably detect false positive and negative threats and attacks; for example, an energy leakage might be detected as energy theft. In the following we list potential artifacts and attributes for monitoring and analyzing in adaptive security and privacy.

Requirements – Requirements can be considered as the reference input (baseline) to the AM. In this way, smart grid security and privacy requirements are presented as runtime entities to be monitored for detecting any requirements denial, frequent denials, conflict, or possibility of not being able to be satisfied anymore. Research work on requirements at runtime, such as requirements-awareness [14], can be useful in monitoring and analyzing requirements for adaptation. Requirements at runtime also enable AM to even modify security requirements, if necessary.

Assets – As noted before, assets should be monitored to track changes in situations similar to Scenario A. An asset is either primary, as the ultimate target of security threats, or secondary, that often needs to be compromised to access related primary assets [7]. A runtime asset model can be useful to track these changes in both asset types, for example in the customer domain, by considering the uncertainty of evaluating assets. By linking such a model to corresponding requirements and conceivable attacks ensuing risk fluctuations can be analyzed. A causal network is useful for this purpose e.g., the fuzzy causal network by Salehie et al. [6].

Context – Due to possible security and privacy ramifications arising from contextual changes, as shown by Scenarios A, C and D, significant contextual attributes should be monitored and analyzed at runtime. A promising approach to considering privacy violation is through the use of contextual integrity framework [15]. This framework posits that different parties should abide by certain transmission principles in the transfer of privacy-sensitive information in each context. For the smart grid, contextual integrity may be a suitable framework, since it represents an explicit model of a sender, receiver and a subject when disclosing personal information, and the transmission principles that guard the interaction process between these entities [16]. Examples of such transmission principles are notice, consent, confidentiality, fiduciary, secrecy, and reciprocity [15].

B. Decision Making

Given perceived security and privacy events, the AM needs to decide how to respond. Making decisions in adaptation is often under uncertainty and deals with multiple objectives.

Risk-adaptation – All security adaptation triggers can be aggregated and presented as risk changes. For example, a causal network can be used to analyze the impact of asset variations on risk and adjust security controls accordingly [6]. The uncertainty of domain experts and incompleteness of evidences can be captured by fuzzy or probabilistic representation of security entities and requirements. Using causal reasoning is also promising in assessing the effect of other changes, such as new vulnerabilities, on risk. The risk-adaptive approach can complement the continuous risk monitoring envisioned by NIST [13].

Privacy Threat Mitigation – Given monitored contextual factors, we should figure out what techniques can be used to reason over ensuing privacy threats. In deciding to adapt, sensitivity of threatened data, history of previous violations, the obfuscation level, and the ability to infer behavioral privacy from disclosed information should be considered. For instance a utility function can be defined based on these factors as a basis for adjusting selective disclosure policies.

Multi-objective Decision-making – Preserving security requires monitoring and tracking details of protected assets, customers' behaviors and meter data. On the other hand, privacy aims to avoid revealing personal information. Therefore, adaptive security and privacy actions can be in conflict. The AM should adapt these two and other quality requirements such as usability and performance. Decision

theory and machine learning techniques may be helpful to address this issue in the smart gird, as they have been in the general adaptive software domain [8].

C. Architecture

IT and ICS – Smart grid architectures are built upon IT and Industrial Control System (ICS) infrastructures. Although these two use different technologies, risk management approaches for them are similar [9]. Vulnerabilities and security controls listed by NIST for ICS [10] are also similar to their IT counterparts. In both, monitoring and auditing need rigorous architectural support for adaptation. Adaptive software architectures need to leverage the NIST continuous monitoring process [13] at runtime, by considering adjustable monitoring and auditing levels to minimize overheads.

Hierarchical Design – Considering the scale of the smart grid, a major challenge is the architecture of AMs and how they communicate with each other. NIST discusses requirements for local and centralized monitoring and control [3]. These requirements and components in the seven designated domains should be considered in arranging adaptation managers in a hierarchical structure. Following the reference architecture of autonomic computing [12], orchestration should be taken into account between security and privacy AMs and other managers for optimizing and healing.

Cloud Architecture – Adopting the cloud architecture for smart grids has an impact on governance, compliance and trust (e.g., data location and ownership). A private or community cloud may be more appropriate to minimize negative effects on privacy and security. But in any selected deployment model, due to numerous parties involved in the grid, adaptation needs to manage access control and auditing in the cloud, among other things. Adaptation is especially required to mitigate risk of multi-tenancy. For example, adaptation manager may identify data items related to customers that need to be migrated to private hosts, if a hybrid cloud model is deployed, to mitigate the risk of data disclosure in multi-tenant hosts. Adaptation should also consider security and privacy concerns in mobile cloud applications.

Human Involvement – Adaptation does not mean that human will not play any role in monitoring, analysis and decision-making in the grid. Due to high level of uncertainty in security and privacy management, and the criticality of assets, a human-in-the-loop and/or on-the-loop styles should be deployed. For example in the former case, a customer is actively involved in reacting to a meter security warning, while in the latter (s)he is simply notified that an action has taken place. In the on-the-loop style, the customer can change the adaptation behavior off-line.

V. Conclusion

Critical cyber-physical assets in the smart grid need to be protected continuously in proactive and reactive ways at run time. Security and privacy requirements, policies and controls may need to be adapted due to possible changes in assets, contextual factors, threats or vulnerabilities. In engineering solutions for adaptive security and privacy in the smart grid, a variety of research issues should be considered in monitoring, decision-making and architecture. Notable research challenges include dealing with uncertainty in monitoring, multi-objective decision-making, and addressing smart grid architecture concerns, such as multi-tenancy in cloud hosts.

Acknowledgment

This work was supported, in part, by Science Foundation Ireland grant 10/CE/I1855 to Lero – The Irish Software Engineering Research Centre (www.lero.ie).

References

1. McDaniel P. and McLaughlin S., "Security and Privacy Challenges in the Smart Grid". IEEE Security and Privacy 7, 3, 75-77. May 2009.
2. NIST, "NIST Framework and Roadmap for Smart Grid Interoperability Standards", Release 1.0, January 2010.
3. NIST, "Guidelines for Smart Grid Cyber Security", NISTIR 7628, Sept 2010.
4. Carpenter M. et al., "Advanced Metering Infrastructure Attack Methodology", InGuardians white paper, Jan 2009.
5. Salehie M. et al., "Towards Self-protecting Smart Metering: Investigating Requirements for the MAPE loop", IEEE Int. Conf. & Workshops on Eng. Autonomic and Autonomous Systems (EASe'12), April 2012.
6. Salehie M. et al., "Requirements-Driven Adaptive Security: Protecting Variable Assets at Runtime", Tech. Rep., Lero-TR-2012-01, 2012.
7. Pasquale L. et al., "On the Role of Primary and Secondary Assets in Adaptive Security: An Application in Smart Grids", Int. Symp. on Software Eng. for Adaptive and Self-Managing Systems (SEAMS), TBA, June 2012.
8. Salehie M. and Tahvildari L., Self-adaptive software: Landscape and research challenges. ACM Trans. Auton. Adapt. Syst. 4, 2, May 2009.
9. Shorter S., Hollenbaugh G., "Automating Smart Grid Security", white paper prepared for NIST, Dec 2011.
10. Stouffer K., Falco J., Scarfone K., "Guide to Industrial Control Systems (ICS) Security", NIST SP800-82, June 2011.
11. Cheng B. et al., "Software Engineering for Self-Adaptive Systems: A Research Roadmap", Self-Adaptive Systems, LNCS 5525, pp. 1–26, 2009.
12. IBM, "An architectural blueprint for autonomic computing", white paper, fourth edition, June 2006.
13. Dempsey K., et al., "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations", NIST SP800-137, September 2011.
14. Sawyer P., et al., "Requirements-Aware Systems- A research agenda for RE for self-adaptive systems", IEEE Int. Requirements Eng. Conf., 2010.
15. Barth, A. et al., "Privacy and Contextual Integrity: Framework and Applications". In Proc of IEEE Symp. on Security and Privacy, 184-198, 2006.
16. Nissenbaum, Helen F., "Privacy as Contextual Integrity", Washington Law Review, Vol. 79, No. 1, 2004.