Adaptive Security in Smart Grid

Raja Ben Abdessalem and Mohamed Hamdi
MEDIATRON Laboratory, Higher School of Communication of Tunis, University of Carthage, Tunis, Tunisia

1 STAGE OF THE RESEARCH

The power infrastructure is being replaced by digital systems based on renewable resources, to meet the growing electricity demand and the gradual depletion of fossil fuels as well as to satisfy the customer's needs in the near future. Smart grid lets users manage, control and predict their energy use. Therefore, the smart grid provides energy efficiency and reduces peak power demand while maintaining resilience, reliability, flexibility and security of the grid (Santacana et al., 2010). Consequently, smart grid should respond rapidly to load changing conditions, reduce the cost of interruptions and power quality disturbances and reduce the probability and impact of attacks.

Smart grid introduces two-way communications where electricity and information can be exchanged between utility and its customers in real-time (NIST,

2010b). However, the expansion of data communication over the power grid, the large number of involved parties and the heavily interconnected communications increase vulnerabilities and raise new security challenges. Potential network intrusion caused by intentional attackers may lead to a variety of damages (Metke and Ekl, 2010).

Moreover, an intrinsic feature of smart grids is that it is at the heart of critical services. In addition to the direct impact that might be generated by the occurrence of an attack, indirect losses can also be taken into account. Therefore, specific security models have to be developed in order to cope with such issues.

This current research aims to develop an adaptive risk-based security framework for smart grid that addresses these security problems taking into account smart grid requirements. The framework will manage data in real-time, estimate risks using game theory approach and apply the appropriate adaptive security decision-making. We mainly focus on analyzing security, privacy risk and requirement capture for adaptive security in smart grid. We also study the existing adaptive security frameworks and to describe their limitations and benefits. We fellow the Design Science methodology (Hevner et al., 2004) to develop a risk-based adaptive framework for the protection of smart grid as well as to develop underlying analytical models.

2 OUTLINE OF OBJECTIVES

The purpose of this thesis is to develop risk-based adaptive security framework for smart grid that will monitor in real-time smart grid environment to detect possible threats, analyze and predict risk damages using game-theory approach. Our framework will adapt security decisions for identified changes using decision-making.

The key objectives of this thesis are:

• Developing the adaptive security monitoring model that uses a continuous cycle of a monitoring framework for smart grid environment, based on the Genetic Message-Oriented Secure Middleware (GEMOM).

• Building models for estimating and predicting risks and benefits using game theory. The thesis will also further improve the accuracy of estimation and prediction mechanisms by applying optimized algorithm for resource allocation.

• Building the adaptive decision-making model that adapt to the dynamic changing conditions of smart grid by selecting the best adaptive security model for a given situation and applying the identified changes.

3 RESEARCH PROBLEM

Smart grid infrastructure might be vulnerable to different forms of threats such as malware, intrusion and Denial of Service (DoS) attacks; The smart grid includes several devices that have two-way

Abdessalem R. and Hamdi M..
Adaptive Security in Smart Grid.

communication with the electric system. These numerous end points, which are located in insecure large scale environments, bring new vulnerabilities. A single vulnerability in a device can be used and exploited to compromise all devices connected to the network. In a smart grid, energy consumption, pricing data and customer information can be vulnerable to attacks. Therefore these critical informations need to be protected. Thus, some security goals need to be achieved and many security parameters should be ensured such as availability, confidentiality and integrity. Many requirements and constraining issues should be considered while designing security techniques and algorithms for the smart grid.

- **Big-data Requirement.** Advanced technologies and application are integrated in the smart grid. Accordingly, a huge amount of privacy-sensitive data will be generated for further control, analysis and real-time pricing methods. These data can be extremely vulnerable to attacks and can be extracted using data mining techniques by different agents such as criminals and insurance companies that determining health care premiums based on customers' life styles. Therefore, it is very critical to define the communication infrastructure requirements to provide a secure and reliable service (Gungor et al., 2011).
- **Resource Limitations.** The smart grid operating systems have unique performance and reliability requirements. The limited availability of computation and communication capabilities makes the security of smart grid more complex. Some smart grid devices have limited bandwidth. However, a significant communication channel is required to ensure the integrity using authentication algorithms. Thus, authentication algorithms should be designed to operate on lower bandwidth channels. Moreover, smart grid devices have limited computational power, memory and storage. This can lead to using weaker security controls. Consequently, the security algorithms and mechanisms should be adapted to these constrained devices.
- **Real-time Requirement.** The smart grid uses a wide area measurement and control to measure the electrical network parameters, to supervise data acquisition and to take decision in real-time. In addition, customers require a real-time transmission of critical information, such as the power consumption, to adjust their consumption and to control peak demand. Customers' personal information (such as their activities, the type of devices used and the energy consumption) can be exposed to various kinds of attacks which can damage customer privacy. Therefore, security algorithms with minimum computational cost should be deployed to ensure the real-time requirement.

Many threats manifests in real-time scenarios. Hence, adaptive security is used to increase awareness and to provide real-time detection and prevention. Adaptive risk management provides automated risk analysis and dynamically adapt to changing conditions. However, most current risk management frameworks that address the security and the privacy problems do not consider these smart grid requirements. Therefore, this current research focuses on the development of adaptive risk management that takes into account the smart grid requirements. This framework will learn, and adapt to changing environment dynamically and will anticipate unknown threats.

4 STATE OF THE ART

In this section, we motivate the need for the risk-based adaptive security, we give brief state-of-the-art in existing privacy and security risk models and we underline their limitations and advantages.

4.1 Adaptive Security

Security and privacy threats manifest in real-time scenarios. Therefore, different vulnerabilities may be introduced to the system. Possible changes might expose the system to new security threats (Salehie et al., 2012). To address these threats, adaptive software models promise to increase awareness, automating monitoring, detection and prevention. Therefore, security controls can be adapted according to the security and privacy requirements' failures at runtime in order to protect critical assets. Adaptive security will check integrity of data if a theft of energy is detected (for example if the energy usage does not much with the reported meter data). In addition, to ensure security controls at runtime, access to the grid's data need adjustment. Adaptive security and privacy aims also to monitor information exchanged to detect possible threats especially in case of mobility where privacy concerns for example user behavior can be revealed. Thus, privacy policies, in such case, need to be adjusted to mitigate possible threats.

4.2 Existing Adaptive Risk Management Frameworks

Traditional security measures such as firewall, Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) usually lack the correlated domain and situational awareness needed to analyze events and inputs. Consequently, they cannot adapt their security postures to evolving situations and transitions.

Risk management provides automated risk analysis by discovering critical assets; realizing their weaknesses and the suitable risk mitigation approaches.

To achieve the vision of a secure smart grid infrastructure, a combined framework for risk management has been proposed in (Riadh W. Y. Habash and Burr, 2013). The risk management framework is used to identify threats and vulnerabilities, to analyze risks and to recommend new controls in order to reduce the risks. This process is periodically repeated to account for changes in the threat situation; and set up policies that address human behavior, which is the basis for all security risks.

Authors in (Ray, 2011) proposed an adaptive risk management framework that exploits near real-time security state and events of power and information systems to adapt security postures of the grid to the situational awareness. Security risks is evaluated using a systematic methodology that consist of identifying all assets (such as power and information systems), assessing vulnerabilities of each asset, analyzing all potential threats that can exploit the identified vulnerabilities, identifying the appropriate security control mechanisms and finally determining the optimum security postures for each asset.

Authors in (Sridhar et al., 2012) proposed a vulnerability assessment framework aiming to quantify risk using Stochastic Petri Nets. The Petri Nets are used to model the cyber network and to obtain the probability of a successful attack. This framework identifies and handles multiple events, then analyzes the risk without providing response strategies. However, Petri nets are facing difficulties in application due to their computational efficiency and scalability (Tang et al., 2004).

4.3 Gap Analysis

Table 1 describes the limitations and the benefits of exiting adaptive risk management frameworks, and the benefits of our proposed framework as comparison as shown in the table below. In this Table, limitations are indicated by ”(-)”, benefits by ”(+)”, ”Req.” (Requirements) indicates the important smart grid requirements and ”Ref.” (References) indicates some existing risk management frameworks.

The risk management of the power grid control information should exploit historical vulnerability and threat data in order to enable domain specific statistical analysis and characterization of attack probabilities and risks.

Following this, we propose a risk-based adaptive security framework using game theory that can model the dynamic behavior of stakeholders. This framework detects in real-time unknown security and privacy threats, respond to them, and adapt to the environment and changing degree of security. The benefits of our proposed framework are presented in Table 1.

4.4 Game Theory

The game theory is widely used to study a variety of security problems (Bier and Azaiez, 2010) (Manshaei et al., 2013). Game theory is a rich mathematical tool that analyzes and models the interaction between an attacker and a defender (the players). The game theory methods can be very useful in improving current risk analysis by clarifying the risks of adversarial situations. The game theory models, that can distinguish clearly between strategic choices and random variable, can make risk assessments more sensible and effective for allocating defensive resources than current risk scoring models (Cox, 2009).

5 METHODOLOGY

5.1 Introducing New Concepts

In this work, we develop a new methodology for dynamic risk assessment based on the approach proposed in (Poslad et al., 2013). The overall adaptive security approach is illustrated in Figure 1.

The synthetic methods are concerned with building models of phenomena related to the development, operation and use of aggregated services, mainly models of software artifacts. We subject to the overall framework of Design Science (Hevner et al., 2004), where information system artifacts are built, and evaluated. Evaluation will be performed using Action Research (Baskerville, 1999), case study research, and formal modelling of

Table 1: Gap analysis of existing risk management frameworks.

Req. / Ref.	Real-time	Resources limitations	Big data
(Riadh W. Y. Habash and Burr, 2013)	(-) The framework does not incorporate attack prevention that accurately predicts future events and adapts accordingly in real-time. (+) The framework is adapted to human behavior by repeating periodically the risk management process.	(-) The unified framework is not optimized since it contains several steps (+) The risk strategy depends on the available resources.	(-) The framework cannot manage a large volume of data.
(Ray, 2011)	(-) The framework does not incorporate attack prevention. (+) The security control posture changes in near real-time in response to changes in the power and information system state changes.	(+) This framework depends on the available resources.	(+) This framework can include data centers and Intelligent Electronic Devices (IEDs) as well as emergent infrastructure and processes.
(Sridhar et al., 2012)	(-) When the number of functional alternative Services increases, many transactions missed their deadlines because they could not get enough resources in time. (+) Petri nets can model the coordination algorithms of the real-time grid transaction and verify their correctness.	(-) Petri nets consume a lot of resources when many services are used.	(+) Petri nets can analyze a large volume of statistics.
Our proposed framework	(+) The adaptive security monitoring model collects data in real-time. (+) SCAP enables sharing metrics and measurements of smart grid in realtime. (+) Our framework incorporates attack prevention to estimate risk in real-time. (+) Our framework enable security control to coordinate with changes in security state and events.	(+) Automated process enables monitoring a larger number of security metrics with few resources and low costs. (+) The predictive model will use an optimized algorithm for resource allocation to choose the best strategy.	(+) Our framework uses SCAP that can monitor a large volume of data.

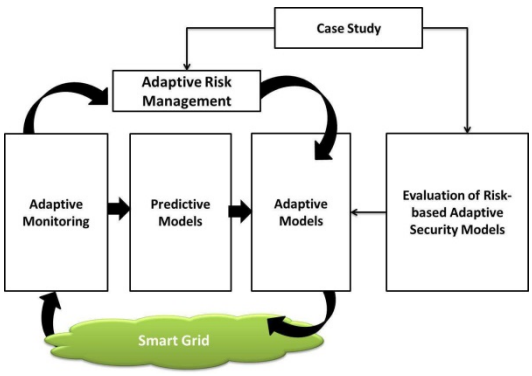

Figure 1: The overall adaptive security approach.

relevant information flows. The methods are also concerned with validating the models using formal criteria and with drawing conclusions from those models. Examples on the use of such methods: Make models based on the formal semantics of programming languages, and analyse the properties of those models, using for example flow analysis to determine flow of information. This leads to sound conclusion using well-established theoretical methods. The security models will be realized as a prototype specification, accompanied with brief guidelines and profiles for use. Additional validation of the design based on formal modelling, will be carried out. The other methods, from software and systems engineering, are used to analyse existing smart grids systems and plan their use.

5.2 Developing, Validating, and Testing New Models

Our proposed framework aims to adapt dynamically the security postures to the changing conditions by monitoring smart grid environment in real-time,

analyzing the collected information (to anticipate unknown threats) and making adaptive decision. Figure 2 illustrates our adaptive risk management framework for smart grid. The framework is composed of three models: the adaptive monitoring model, the predictive model and the adaptive decision model.

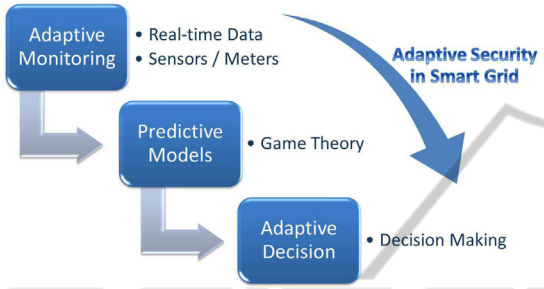

Figure 2: Adaptive risk management framework for Smart Grid.

5.2.1 Adaptive Monitoring

The adaptive security monitoring model collects data in real-time from different devices such as meters and sensors. However, the interoperability among them is a critical requirement to integrate security and risk mitigation. In this context, the National Institute of Standards and Technology (NIST) developed a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems (NIST, 2010a). Authors in (DHS, 2011) proposed three interdependent building blocks to enhance cybersecurity: interoperability, automation and authentication. Interoperability defines cyber communities by policies which permit to cyber participants to collaborate dynamically in automated community defense. Automated process enables monitoring a greater number of security metrics with fewer resources, lower cost and greater reliability and efficiency than using manual process. Automated monitoring provides measurable, relevant and timely information. Many technical security controls can be used for monitoring with automated tools. Automated tools, such as Security Content Automation Protocol (SCAP) (Barrett et al., 2009), help monitoring large volumes of data. SCAP is used to communicate data in a standardized format for performing security automation capabilities and promoting interoperability of security products. SCAP integrates the Common Vulnerability Scoring System (CVSS) and Common Vulnerabilities and Exposures (CVE) in order to provide quantitative and repeatable measurement and scoring of software flaw vulnerabilities across system. The standardization makes security metrics and measurements easier to share. In order to ensure an up-to-date threat and vulnerability knowledge in the smart grid system, we propose to use shared metrics and measurement repositories such as SCAP.

Our adaptive security monitoring will use a continuous cycle of a monitoring framework for smart grid environment, based on the Genetic MessageOriented Secure Middleware (GEMOM). GEMOM, which was proposed in the European Commission's Framework Programme 7 project GEMOM (2008-

2010), develops a messaging platform that is resilient, evolutionary, self-organizing, self-healing, scalable and secure (Abie et al., 2009).

5.2.2 Predictive Model

The predictive model uses the monitored information to estimate and predict risks based on game theory approach. The game theory is suitable for modeling and analyzing the complexity of interaction between stakeholders and adversaries as well as their behaviors and the choice of their strategies. However, the players' strategies can include allocations of resources to prepare for possible attacks. The predictive model will use an optimized algorithm for resource allocation to choose the defender's best allocation of defensive resources, taking into account the attacker's best response.

5.2.3 Adaptive Decision

Adaptive decision model will enable security control to coordinate with changes in security state and events. The resulting predictive model helps smart grid to take decisions on their security strategies while considering their resource constraints.

Adaptive security decision-making will adapt security control according to the level of security and the role of stakeholders.

6 EXPECTED OUTCOME

The proposed risk management framework ensures an adaptive security for smart grid by monitoring data in real-time, predicting risks and adapting

security decisions to changing circumstances. Our framework is based on a continuous cycle of adaptive monitoring, predictive analytics and automated adaptive decisionmaking. In our future work, we aim to develop the adaptive monitoring model using automated process and based on the GEMOM Middleware. Then, we plan to develop the predictive model that will estimate risks and the decision-making model.

REFERENCES

Abie, H., Savola, R., and Dattani, I. (2009). Robust, secure, self-adaptive and resilient messaging middleware for business critical systems. In *Future Computing, Service Computation, Cognitive, Adaptive, Content, Patterns, 2009. COMPUTATIONWORLD '09. Computation World*:, pages 153–160.

Barrett, M., Johnson, C., Mell, P., Quinn, S., Scarfone, K. Stephen Quinn, K. S. M. B., and Johnson, C. (2009). *Guide to adopting and using the Security Content Automation Protocol (SCAP)*. NIST Special Publ. 800-117 (Draft), U.S. National Institute of Standards and Technology.

Baskerville, R. L. (1999). Investigating information systems with action research. *Commun. AIS*, 2(3es). Bier, V. M. and Azaiez, M. N. (2010). *Game Theoretic Risk Analysis of Security Threats*. Springer.

Cox, Jr., L. A. T. (2009). Game theory and risk analysis. *Risk Analysis*, 29(8):1062–1068.

DHS (2011). *Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*. DHS National Protection and Programs Directorate.

Gungor, V., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., and Hancke, G. (2011). Smart grid technologies: Communication technologies and standards. *Industrial Informatics, IEEE Transactions on*, 7(4):529–539.

Hevner, A. R., March, S. T., Park, J., and Ram, S. (2004). Design science in information systems research. *MIS Q.*, 28(1):75–105.

Manshaei, M. H., Zhu, Q., Alpcan, T., Bacs¸ar, T., and Hubaux, J.-P. (2013). Game theory meets network security and privacy. *ACM Comput. Surv.*, 45(3):25:1–25:39.

Metke, A. and Ekl, R. (2010). Smart grid security technology. In *Innovative Smart Grid Technologies (ISGT)*, 2010, pages 1–7.

NIST (2010a). Nist framework and roadmap for smart grid interoperability standards, release 1.0.

NIST (2010b). The smart grid interoperability panel-cyber security working group: Smart grid cyber security strategy and requirements. *NIST IR-7628*.

Poslad, S., Hamdi, M., and Abie, H. (2013). Adaptive security and privacy management for the internet of things (aspi 2013). In *Proceedings of the 2013 ACM Conference on Pervasive and Ubiquitous Computing Adjunct Pub*lication, UbiComp '13 Adjunct, pages 373–378, New York, NY, USA. ACM.

Ray, P. D. (2011). Interoperating grid cyber security systems: Adaptive risk management across unified ot and it domains. *Grid-InterOp*.

Riadh W. Y. Habash, V. G. and Burr, K. (2013). Risk management framework for the power grid cyber-physical security. *British Journal of Applied Science and Technology*.

Salehie, M., Pasquale, L., Omoronyia, I., and Nuseibeh, B. (2012). Adaptive security and privacy in smart grids: A software engineering vision. In *Software Engineering for the Smart Grid (SE4SG), 2012 International Workshop on*, pages 46–49.

Santacana, E., Rackliffe, G., Tang, L., and Feng, X. (2010). Getting smart. *Power and Energy Magazine*, IEEE, 8(2):41–48.

Sridhar, S., Govindarasu, M., and Liu, C.-C. (2012). Risk analysis of coordinated cyber attacks on power grid. In *Control and Optimization Methods for Electric Smart Grids*. Springer New York.

Tang, F., Li, M., and Huang, J. Z. (2004). Real-time transaction processing for autonomic grid applications. *Eng. Appl. Artif. Intell.*, 17(7):799–807.