Smart grid cyber-security standards: today and tomorrow

Mr Thomas Bleier*, Dr Lucie Langer, Dr Florian Skopik, and Dr Paul Smith
AIT Austrian Institute of Technology, 2444 Seibersdorf, Austria
*Tel: +43(0) 664 8251279; Fax: +43(0) 50550-2813; Email: thomas.bleier@ait.ac.at

Abstract

Smart grids include a significant Information and Communications Technology (ICT) component, which is used to support advanced services, such as demand-response management. With this increased use of ICT, there is a greater risk from cyber-attacks. Appreciating this, a number of organisations have developed standards and recommendations for securing smart grids. In this poster, we present an overview of existing standards for securing smart grids, and point to areas in which further effort is required, e.g., for cyber-security information sharing across smart grid stakeholders.

1 Cyber-security: today

International standards bodies and related organisations have developed a number of standards, guidelines and recommendations for smart grid cyber-security. We briefly summarise prominent contributions.

NIST-IR 7628 Guidelines: The U.S. National Institute of Standards and Technology (NIST) has developed a three-volume report on "Guidelines for Smart Grid Cyber Security" [1]. Volume one defines a high-level architecture, categorising the interfaces in a smart grid, and presents an approach to identifying security requirements for these interface categories. Volume two focuses on privacy risks – an important consideration in smart grids – that arise in customer premises. It gives high-level recommendations on mitigating these risks. Volume three provides supporting material, such as classes of potential vulnerabilities for the smart grid. Arguably, the NIST-IR 7628 guidelines represent seminal work in this area, on which further recommendations have been developed.

ENISA Smart Grid Security Recommendations: The European Network and Information Security Agency (ENISA) has issued two reports on smart grid security: The first gives ten high-level recommendations to the public and private sector, and is primarily aimed at raising awareness of smart grid security issues [2]. The recommendations are based on a survey of fifty smart grid experts and stakeholders. The second report provides a set of more specific measures for smart grid service providers, aimed at establishing a minimum level of cyber-security [3]. The measures are organised into ten domains, covering different security aspects, such as risk management, incident response or physical security. Each security measure can be implemented at three different levels of sophistication, ranging from early-stage to advanced. It builds on existing work like NIST-IR 7628 or ISO 27002.

CEN-CENELEC-ETSI Framework: In 2011, the CEN-CENELEC-ETSI Smart Grid Coordination Group was formed, in order to provide a comprehensive framework on smart grids [4], in response to the EU Smart Grid Mandate M/490. The framework consists of several reports that are relevant for cyber-security: The "First Set of Standards" provides a list of standards to be considered for an efficient deployment of smart grids in Europe, including an overview of the current cyber-security standardisation landscape. The "Smart Grid Reference Architecture" defines a three-dimensional technical reference architecture, which also provides a method to analyse information security use cases in smart grids. The "Sustainable Processes" report contains a list of high-level use cases that represent characteristic smart grid operation. They provide a basis for further cyber-security developments, such as information security risk analysis. Finally, the "Smart Grid Information Security" report provides cyber-security requirements and implementation recommendations. It defines security levels to bridge the gap between electrical grid operations and information security, and provides related data protection levels to classify data in the grid, and matching protection requirements.

BSI Protection Profile: Directly considering a key system component in a smart grid, the German Federal Office for Information Security (BSI) has created a Common Criteria Protection Profile for the "Gateway of a Smart Metering System and its Security Module": BSI-CC-PP-0073 [5]. A corresponding certification will become mandatory for smart metering devices that are deployed in Germany [6]. It is accompanied by another Profile, BSI-CC-PP-0077 [7], specifying the security requirements for the security module, which provides cryptographic support. Furthermore, Technical Guidelines provide implementation guidance for the Protection Profiles.

ISO/IEC 27019: The upcoming ISO/IEC 27019 standard [8] defines a management framework for implementing an information security management system (ISMS) for energy utilities. It is based on the general ISO/IEC 27002 standard for implementing an ISMS. As a specialisation of this standard, ISO/IEC 27019 specifies a Deming-Cycle (Plan-Do-Check-Act) process for the implementation of information security. Based on a risk assessment, a hierarchical structure of policies for implementing information security measures is defined. The 27002 standard provides ten domains to consider, with general recommendations, and the 27019 standard provides extensions and clarifications for the specific environment of the energy sector. Organisations implementing such an ISMS can be certified according to the ISO/IEC 27001 standard.

2 Cyber-security: tomorrow

The discussed smart grid cyber-security standards represent important and necessary work. However, we argue they do not represent the complete picture and important pieces are still missing. We discuss two critical areas in which further effort is needed: *cyber-security information sharing* and *resilience*.

Cyber-security information sharing: Attacks are becoming increasingly sophisticated, targeted, and coordinated [9]. Therefore, we need new paradigms for detecting them in complex connected systems, such as the smart grid. Currently, many attack detection tasks are performed within a single organisation. We argue that cross-organisational security information sharing is a crucial step to correctly understand large-scale cyber-attack situations, and to warn others against threats. However, in practice, security information sharing is usually accomplished via ad-hoc and informal relationships [10]. Often, national Computer Emergency Response Teams (CERTs) assume the role of a contact point for coordinating and aggregating security incidence reports. However, the information that is provided is usually not targeted to particular vertical industry sectors, such as power grids. We suggest that, in order to make such platforms more effective, *sector-oriented views*, along with *rich information and experience reports* are required. Furthermore, there is a crucial trade-off to be considered: existing platforms require information to be verified centrally (in order to avoid hoaxes); therefore, the speed of information distribution suffers. Timeliness of information is very important when protecting against aggressive attackers and zero-day exploits. Consequently, we foresee a need for new standards that employ *suitable direct sharing models*, which allow the targeted exchange of specific information about discovered vulnerabilities of ICT systems utilised in the smart grid, as well as current threats (such as new SCADA-targeted malware) and recent incidents. The application of these standards further implies the existence of a *federated trust and reputation model* to address reservations of users, and to attract a critical mass of users.

Smart grid resilience: Closely related to issues of cyber-security information sharing are *resilience* aspects [11]. The assumption when considering resilience is that, inevitably, attackers will be successful and a system must continue to provide a service, or degrade gracefully – an important property of a smart grid. To achieve this, a number of items could be standardised and guidelines drawn up: fundamentally, it will be necessary to measure the resilience of a smart grid; suitable *metrics*, which relate in the power systems and ICT domains, are required for this, along with supporting analysis methods and tools. *Architectures* (and design guidelines) for smart grid resilience need to be developed that account for potential failures of security components, which are fault-tolerant and provide modes of operation that are potentially degraded but, most importantly, safe. Another example area in which guidelines could have significant benefit is *processes* for resilience: implementing resilience will involve coordinating a number of (increasingly) automatic and manual processes that implement different stages of a resilience strategy, i.e., from detecting a problem to implementing some remedial actions. Whilst each incident is likely to be subtly different, templates for resilience, in the form of so-called *patterns*, which can be instantiated when necessary, could expedite the implementation of resilience strategies. Arguably, these aspects are not well addressed in current standards and recommendations.

3 Conclusion

We have briefly surveyed the smart grid cyber-security standardisation landscape, and identified key areas in which we believe additional standards and guidelines are required for a secure *and* resilient smart grid. We are investigating these aspects together with a number of European partners in on-going work in the context of the Austrian nationally-funded $(SG)^2$ project and forthcoming EU-funded SPARKS project. Results of our work are targeted towards the aforementioned international bodies.

4 References

[1] The Smart Grid Interoperability Panel "Cyber Security Working Group: Guidelines for Smart Grid Cyber Security," Vol. 1-3, 2010.

[2] European Network and Information Security Agency (ENISA): "Smart Grid Security: Recommendations for Europe and Member States," July, 2012.

[3] European Network and Information Security Agency (ENISA): "Appropriate security measures for smart grids," December 2012.

[4] CEN-CENELEC-ETSI "Smart Grid Coordination Group, Reports in response to Smart Grid Mandate M/490," 2012.

[5] Federal Office for Information Security, "Protection Profile for the Gateway of a Smart Metering System, V.1.2," March, 2013.

[6] K. J. Müller, "Verordnete Sicherheit - das Schutzprofil für das Smart Metering Gateway - Eine Bewertung des neuen Schutzprofils," Datenschutz und Datensicherheit, Vol. 35, No. 8, pp. 547–551, 2011

[7] Federal Office for Information Security, "Protection Profile for the Security Module of a Smart Metering System, V.1.0," March, 2013.

[8] ISO, "ISO/IEC TR 27019:2013: Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry," 2013.

[9] C. Tankard, "Advanced persistent threats and how to monitor and deter them," Network Security, Vol. 2011, No. 8, pp. 16–19, 2011.

[10] U.S. Homeland Security Cyber Security R&D Center, "A roadmap for cyber security research," November 2009.

[11] James P.G. Sterbenz et al., "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," Computer Networks, Vol. 54, No. 8, June 2010, pp. 1245-1265.