Enabling Security-by-design in Smart Grids: An architecture-based approach

Helder Aranha
Information Systems Department
ESPAP, I.P.
Alfragide, Portugal
helder.aranha@espap.pt

Massimiliano Masi
Tiani Spirit GmbH
Vienna, Austria
massimiliano.masi@tiani-spirit.com

Giovanni Paolo Sellitto
Independent Scholar
Rome, Italy
gogiampaolo@gmail.com

and
Tanja Pavleska
Laboratory for Open Systems and Networks
Jozef Stefan Institute
Ljubljana, Slovenia
atanja@e5.ijs.si

***Abstract*—Energy Distribution Grids are considered critical infrastructure, hence the Distribution System Operators (DSOs) have developed sophisticated engineering practices to improve their resilience. Over the last years, due to the ”Smart Grid” evolution, this infrastructure has become a distributed system where prosumers (the consumers who produce and share surplus energy through the grid) can plug in distributed energy resources (DERs) and manage a bi-directional flow of data and power enabled by an advanced IT and control infrastructure. This introduces new challenges, as the prosumers possess neither the skills nor the knowledge to assess the risk or secure the environment from cyber-threats. We propose a simple and usable approach based on the Reference Model of Information Assurance & Security (RMIAS), to support the prosumers in the selection of cybesecurity measures. The purpose is to reduce the risk of being directly targeted and to establish collective responsibility among prosumers as grid gatekeepers. The framework moves from a simple risk analysis based on security goals to providing guidelines for the users for adoption of adequate security countermeasures. One of the greatest advantages of the approach is that it does not constrain the user to a specific threat model.**

***Index Terms*—Smart Grids, security-by-design, methodology, architecture, RMIAS**

I. Introduction

Establishing the Smart Grid requires coordination of several distributed energy resources (DERs), which are hosted either at power plant facilities (e.g., offshore wind turbines) or at prosumer dwellings (e.g. a solar panel). Dealing with privately owned power sources and distributed micro-production (and now micro-storage) is a daily challenge for grid operators such as Distributed System Operators (DSOs). DSOs have to deal with a growing number of volatility factors, balancing demand and supply that can vary abruptly and independently in space and time, while maintaining grid stability. Article 4 of the NIS directive, (EU) 2016/1148 lists the Energy production Sector under Critical infrastructures, mandating high standards of cybersecurity countermeasures to protect the assets [1]. While Smart Grid teams involve cybersecurity experts, the same cannot be stated about the DERs side, especially in the case of households with small/medium voltage contribution. Nevertheless, by participating in the grid they hold part of the control system that may expose the household, as well as all the Smart Grids it is part of, to unknown cybersecurity threats: grid power instability, malware spreading, and user profiling based on the energy consumption, to name a few. A whole new cybersecurity context emerges from these premises, which must be accounted for by both the Smart Grid operator and the DER owners. Best security practices usually move from the definition of a threat model (for e.g., according to a standard list) and look for adequate countermeasures. However, for a threat model to be established, statistics and history of functional behaviors of the system are needed, including knowledge of both existing and potential attackers. Such information is often unavailable, especially when novel systems are designed or new components are added to an existing one. In any case, prosumers rarely have the capabilities to envisage the threats and to protect their end of the grid. Other approaches are too generic to scale to the decentralized model of the Smart Grid [2].

To cater for the cybersecurity needs of the prosumers and to avoid being constrained to a specific threat model, we adopt a bottom up approach to Information Assurance and Security (IAS), proposing a framework based on several methodological tools, the main pillar of which is the Reference Model for Information Assurance and Security - RMIAS [3]. RMIAS identifies four security aspects (dimensions) of an information system: Life Cycle, Information Taxonomy (Classification), Security Goals and Countermeasures. It is goal-based and, unlike threat modelling, it requires a set of security objectives to be met in order to establish the security methodology needed to address them. Security objectives can be envisaged by business people, since they only require an assessment of the existing assets and an analysis of their value. A bottom up approach fits well in the context of Smart Grids, where both NIST and the EU Commission promote the use of modular

978-1-7281-3929-6/19/$41.00 ©2019 IEEE
DOI 10.1109/EDCC.2019.00042

architecture. The Smart Grid Architecture Model (SGAM) [4] introduces the concept of Basic Application Profile (BAP) [5] as a way to address this requirement. However, SGAM does not provide a methodology to define BAP interactions, which is crucial for assessing *ex-ante* the risk related to injecting new (potentially malicious) components into the grid. In order to fill this gap, we consolidate SGAM with a process that has already been adopted in another critical sector, e-Health. This process is known as Integrating the Healthcare Enterprise (IHE) [6]. By providing a full formal account of the IHE process we offer a toolchain that facilitates a plug and play approach to DER solutions in the Grid and offers automated evaluation of the DER security properties, thus supporting the grid's evolving configuration.

The remainder of the paper is organized as follows: Section II presents the rationale for merging IHE with the SGAM model in view of the architectural requirements and modelling specifications. Section III outlines the proposed approach and joins together the cybersecurity (through RMIAS) and the Smart Grid system design principles. Related work is overviewed in Section IV to position our proposal among the state of the art approaches. Section V concludes with ongoing and future steps for methodological formalization and validation.

II. Evaluating security-by-design in Smart Grids

SGAM enables a modular architecture where single premade components could, in principle, be easily combined, checked and turned into software products, reducing time-to-market and lowering the adoption barriers for prospective DER owners. A current limitation is that building solution architectures based on SGAM is a fully manual task: the architect must select the adequate architectural constructs, evaluating all the interdependencies among them and considering all variability points within each construct in order to provide a cohesive and interoperable solution. In addition, while SGAM accounts for cybersecurity and privacy in Smart Grids from standardization aspect (refer to CG-SEG report in [7]), it lacks a generic (context independent) methodology to facilitate the enforcement of adequate security levels.

The e-Health sector has experienced similar issues; patients' electronic health records are shared among hospitals in different regions, speaking different languages, having different security requirements. A stolen patient record poses serious privacy issues and, if misused, even endangers the patient's life.

IHE [6] offers a complete lifecycle methodology consisting of: i) a set of rules to select candidate standards to fulfill clinical use cases, ii) a process which deals with the evolution of the standards, iii) a model to amend existing publications, and iv) a method to provide interoperability and conformance testing. IHE architectural model is modular: at the core of each *technical framework* lie the concepts of *actor* (a functional component of the healthcare organisation) and *transaction* (a standards-based specification of the interactions between actors). In addition, an *integration profile* is a high-level functional unit composed of related IHE transactions, addressing specific IT infrastructure requirements for a single use case. A profile can include functional dependencies from other profiles (expressed as *grouping rules*) and can exhibit optionality/variability as its traits. By employing the grouping rules the architect knows which profiles are optionally or mandatorily interconnected.

Our methodology stems from a side-by-side analysis of the SGAM with the solution that engineers in the e-Health sector found for the problem of establishing and securing an interoperable e-Health network. We enhance SGAM with those findings to build a generic solution for the Smart Grids domain. To do that, we propose to support this combined IHE-SGAM modular architecture with a RMIAS-based security model in order to provide a fully automated methodology capable not only for building Smart Grid architectures, but also for automatic evaluation of their quality attributes and security properties. The proposal thus empowers the architect with a toolchain that enables continuous validation of the resulting architecture and an ex-ante evaluation of any additional components. Automating the toolchain by exploiting a fully implemented formal language encourages such test-driven architectural design approach.

Next, we present the integration of IHE, SGAM and RMIAS into the novel approach.

III. Enabling automated evaluation of security properties

In addition to basing the conceptual framework on the state of the art approaches, such as RMIAS and SGAM, the practical implementation of our proposal builds on the pragmatic foundations provided by important EU Large Scale Pilots, such as e-SENS[1] and the IES initiative[2]. Both SGAM and IHE treat cybersecurity as a cross-cutting concern. In IHE, this concern is reflected in the grouping rules: a baseline security profile (ATNA) is a mandatory dependency for all profiles. However, being a continuously evolving field, the approaches that deal with security issues must be adapted accordingly. We formalized our combined SGAM-IHE model in an earlier work [8]. Now, we extend it with the Reference Model of Information Assurance & Security (RMIAS) [3], which results in a multidimensional framework for Information Assurance and Security. Furthermore, in [8] we introduced an architecture description language (ADL) to be used by the architect to **(a)** describe architecture building blocks (i.e. profiles), **(b)** specify interactions among them, and **(c)** semi-automatically create input to verify the fulfillment of quality constraints with formal methods. Within the new framework, we extend this ADL with RMIAS-based notions and we call the result *MOdular Security-Aware ADL*, MOSA[2].

According to our conceptual framework, architects would start by defining the architectural profiles and specifying

[1] http://www.esens.eu

[2] http://iesaustria.at

quality attributes by using MOSA^2 constructs, as described in **(a)(b)(c)** and elaborated broadly in [8]. Then, they would add modular security requirement (sub)constructs into the architecture itself, by following the RMIAS process: per profile, identifying information assets to protect with the help of well-defined taxonomies; mapping the former into information categories; performing risk analysis to prioritize the security goals deemed appropriate for each category according to business needs; and ultimately, identifying and selecting cost-effective security countermeasures to fulfill the security goals for each category.

As part of our empirical (practical) framework, a fully automated process guided by a formal semantic model builds the code to be used for further analysis, but also for specifying the evaluation protocol. The latter is done using SMT-LIB[3]. We then employ the Z3 solver[4] to provide a formal proof for supporting the architecture security goals. By iterating through this process, the architect *refactors* the architecture while having a formal proof at all times on whether the security goals and the quality service level agreements are met by design.

The RMIAS-based process described above (finding the best countermeasures an organization can afford to protect important information assets from identified categories of cyberthreats), portrays itself as fully embedded in the IHE-SGAM hybrid architectural process. Moreover, it is equally applicable and amendable to SGAM-based architectural processes that do not necessarily embrace modularity to design Smart Grid functionalities. MOSA^2 leverages this approach into modular architectural constructs to allow for automated security evaluation. The language is implemented and available at http://github.com/mascanc, including the full account of the IHE framework and the IHE-SGAM hybrid IES technical framework to establish a VPP.

IV. Related Work

Mandated by the European Commission, the joint group CEN-CENELEC-ETSI introduced SGAM to provide a holistic architectural view on Smart Grids. SGAM is meant as an enabler for establishing Smart Grids in Europe, which the member states and the individual projects are encouraged to follow [9]. Adopting such an architectural model is crucial not only to fulfill the Availability of a resource (DER in our case), but also to avoid the effect of *vendor lock-in*.

In addition to being Smart Grids oriented, our work is also a contribution to the field of architectural description languages (ADLs). In that sense, the works that come closest to ours are [10] and [11]. The latter introduces PSAL, a domain-specific language to build SGAM-based solutions. Our approach differs in several ways: we provide a formal account of the language; we specifically devise constructs to address security-by-design; we provide constructs to account for completeness by implementing profile grouping rules, a central feature of the IHE framework. In the context of architectural models, approaches similar to ours have also been proposed[5]. However, they follow the typical modular approach of the enterprise architecture[6], defining functionalities and architectural assets ”wrapped” by specific containers named *building blocks* (in our approach interchanged with the concept of profiles) and a composition method to build a *solution* architecture. Our approach does not only belong to the Energy domain - it can be shared among different verticals[7].

V. Future Work

The implementation of MOSA^2 is an ongoing activity, which should provide a formal proof in terms of validation of the stated results and contributions. In our future work, we will enhance the language constructs with a visual editing tool that will enable the architect to group the profiles and immediately observe their dependencies. Moreover, we will formalize the RMIAS clauses to allow for practical and adaptable implementation in building secure-by-design systems.

References

[1] The European Parliament and the Council of European Union, “Directive (EU) 2016/1148,” 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

[2] D. Dolev and A. C. Yao, “On the security of public key protocols,” in *Proceedings of the 22Nd Annual Symposium on Foundations of Computer Science*, ser. SFCS ’81. Washington, DC, USA: IEEE Computer Society, 1981, pp. 350–357. [Online]. Available: https://doi.org/10.1109/SFCS.1981.32

[3] Y. Cherdantseva and J. Hilton, “A Reference Model of Information Assurance & Security,” in *2013 International Conference on Availability, Reliability and Security*, Sep. 2013, pp. 546–555.

[4] Smart Grid Coordination Group, “Smart Grid Reference Architecture,” CEN-CENELEC-ETSI, Technical Report, Nov. 2012.

[5] SG-C/M490/I_Smart Grid Interoperability, “Methodologies to facilitate Smart Grid system interoperability through standardization, system design and testing,” CEN, CENELEC, ETSI, Standard, Oct. 2014.

[6] Integrating the Healthcare Enterprise, “The IHE IT Infrastructure Technical Framework,” IHE, Standard, Nov. 2019.

[7] SG-CG/M490/, “Smart Grid Information Security,” CEN, CENELEC, ETSI, Standard, Dec. 2014.

[8] M. Masi, T. Pavleska, and H. Aranha, “Automating Smart Grid Solution Architecture Design,” in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2018, Aalborg, Denmark, October 29-31, 2018*. IEEE, 2018, pp. 1–6. [Online]. Available: https://doi.org/10.1109/SmartGridComm.2018.8587457

[9] M. Gottschalk, M. Uslar, and C. Delfs, *The Use Case and Smart Grid Architecture Model Approach: The IEC 62559-2 Use Case Template and the SGAM Applied in Various Domains*, 1st ed. Springer Publishing Company, Incorporated, 2017.

[10] F. P. Andrén, T. I. Strasser, and W. Kastner, “Engineering smart grids: Applying model-driven development from use case design to deployment,” *Energies*, vol. 10, no. 3, 2017. [Online]. Available: https://www.mdpi.com/1996-1073/10/3/374

[11] T. I. Strasser, S. Rohjans, and G. M. Burt, “Methods and Concepts for Designing and Validating Smart Grid Systems,” *Energies*, vol. 12, no. 10, pp. 1–5, May 2019. [Online]. Available: https://ideas.repec.org/a/gam/jeners/v12y2019i10p1861-d231521.html

[3] We use the SMT-LIB specifications since they are standard and adopted by most of the SMT solvers available.

[4] See https://github.com/Z3Prover/z3

[5] E.g. the NIST Smart Grid Framework, https://www.nist.gov/engineering-laboratory/smart-grid/smart-grid-framework and OpenADR, https://www.openadr.org/specification

[6] See for e.g. https://www.opengroup.org/togaf

[7] https://ec.europa.eu/digital-single-market/en/news/new-version-european-interoperability-reference-architecture-available, https://ec.europa.eu/isa2/eif_en