SealedGRID: A Secure Interconnection of Technologies for Smart Grid Applications

Aristeidis Farao[1], Juan Enrique Rubio[2], Cristina Alcaraz[2], Christoforos Ntantogian[3], Christos Xenakis[3], and Javier Lopez[2]

[1] Neurosoft S.A., Athens, Greece
a.farao@neurosoft.gr
[2] Computer Science Department, University of Malaga
Campus de Teatinos s/n, 29071,Malaga, Spain
{rubio,alcaraz,jlm}@lcc.uma.es
[3] Department of Digital Systems, University of Piraeus, Greece
{dadoyan,xenakis}@unipi.gr

Abstract. In recent years, the Smart Grid has increasingly integrated cutting-edge technologies that generate several benefits for all the stakeholders involved, such as a more accurate billing system and enhanced Demand Response procedures. However, this modernization also brings with it diverse cyber security and privacy issues, which sets the necessity for developing a security platform specifically tailored to this scenario. In this paper, we present SealedGRID, which proposes a flexible architecture that provides security services at all levels by implementing Trusted Execution Environments on their devices, together with advanced authentication and authorization mechanisms, as well as privacy preserving techniques. These technologies are presented in depth and a final security analysis is conducted, which highlights the contributions of this project.

Keywords: Smart Grid · Interoperability · Trust · Scalability.

1 Introduction

The rapid evolution of Information and Communications Technologies (ICT) has fostered the evolution of traditional power grids to the Smart Grid (SG). It supports a two-way information exchange between customers and the Utility companies that enables a sustainable energy management and flexible tariffs that result in lower bills. EU regulations require member nations to ensure that 80% of residential households will be fitted with Smart Meters (SM) by 2020. However, the power grid will be also exposed to security threats inherited from the ICT sector, while privacy issues and new vulnerabilities related to the specific characteristics of the SG infrastructure will emerge. In this context, This paper highlights the main contributions of the SealedGRID project for the protection of the SG against these and other sophisticated attacks, providing a scalable, highly trusted, and interoperable SG security platform. It is applicable to modern industrial networks as well as traditional control infrastructures like SCADA and telemetering systems, abiding the existing standardization work.

The architecture of this solution complies with the following requirements:

- **Scalability**: concerning the protection of utilities, which are vulnerable target due to the centralization of the grid
- **Trust**: SG nodes will be accessible by customers creating a fertile field for malicious users that may intercept personal information or alter energy measurements and costs;
- **Interoperability**: multiple heterogeneous technologies with multiple network operators and other stakeholders are involved.

In the next paragraphs, we present an overview of state-of-the-art technologies used in SealedGRID. Beginning with **key management**, some schemes in the SG are based on shared secret keys, which in turn hinder scalability. Other schemes utilize ID-based cryptography [1], whose main issue is that Private Key Generator should always be online and available, being a single point of failure.

There have also been efforts to integrate **trusted computing** on the SG, mainly with the use of the Trusted Platform Modules (TPM) [2] and the Trusted Execution Environments (TEE) [3]. In this project, we prioritize the use of TEEs, since TPMs usually imply higher costs, they do not offer protection against runtime attacks, they are not suitable for embedded devices and do not provide runtime attestation of executable programs; which can be met on the TEE and are required by the SealedGRID concept.

Regarding **privacy**, a lot of research has been done to prevent data disclosure by means of cryptography, using homomorphic encryption, traditional encryption, and masking. Based on standardization organizations in [4], the efficiency and privacy requirements of a privacy preserving mechanism for the SG can be met using masking. Solutions like [5] lack protection against non-repudiation and adaptability to node joining or leaving.

Authentication is also an important issue by the industry, leading to standards like DNP3 Authentication [6] and IEC 62351-5 [7]. In [8], a device-to-device authentication framework based on a two-layer approach is presented, where SMs are authenticated globally by a PKI and locally by channel signatures. In [9], an authenticated aggregation protocol is presented based on asymmetric keys, which preserves the authenticity of exchanged messages.

The design of secure **authorization** and interoperability mechanisms is also complex task [10], since the inter-connection between systems that are not originally envisioned to interoperate may present unanticipated problems. In [11], authors propose a dynamic authorization-based architecture based on Role Based Access Control, Policy Enforcement Points (PEPs) and Policy Decision Points (PDPs) to collect data streams from multiple sources connected to the Advanced Metering Infrastructure. Lastly, [12] presents a solution based on the use of PEPs and PDPs to interconnect large distributions with different vendor technologies.

The rest of the paper is organized as follows: Section 2 presents the different technologies used in SealedGRID, whereas Section 3 describes how they are integrated by the different components of its architecture. Section 4 analyzes how SealedGRID solutions address certain operational and security requirements, concludes the paper and adds the future work.

2 SealedGRID Technologies

In this section we briefly present the applied technologies in the proposed SealedGRID architecture which are the following: a) Federated Login [13]; b) SOMA [14]; c) MASKER [15]; d) TEE [16] and e) Context Awareness Manager [17].

The SealedGRID deploys **Federated Login** achieving interoperability and ensuring communication among its components. Then, it utilizes OpenID Connect and OAuth2.0. However, we will not analyze these technologies, since they preexist the SealedGRID and are borrowed from the field of online services, [13].

SOMA [14] is a certificate-based authentication infrastructure that creates a secure authentication system for mesh networks without a TTP. It creates an efficient, self-organized and scalable authentication infrastructure based on a PGP-like architecture. The nodes independently decide with whom to interact, since the SOMA is built on a Peer-to-Peer (P2P) and Web-of-Trust (Wot) infrastructure. This way, SOMA does not use a Credential Authority (CA) and avoids delegation of trust to a TTP. Moreover, SOMA demands the existence of TEE for its secure execution and storage of the generated certificates.

MASKER [15] provides a privacy-preserving aggregation solution that responds to the following issues: a) it assists the privacy and security of energy consumer and b) facilitates DR. The SMs share cryptographically generated pseudo-random values with the Utility. These act as masks and obfuscate the real SMs consumption readings; an intermediate Aggregator provides the Utility with an aggregated consumption by several SMs. The Utility subtracts the used masks from the received sum, resulting the real combined consumption. Only, the SM has access to its real energy consumption value. All sensitive computations are protected by a TEE, which stores data and executes crucial operations.

As mentioned above, SealedGRID uses a **TEE** to protect its components from being manipulated and achieve these goals: a) to protect device private keys and its sensitive data through secure storage; b) to endorse remote attestation, and c) to secure critical procedures like key management. Particularly, SOMA is executed within the TEE, where its certificates are stored. Furthermore, MASKER utilizes the TEE to provide confidentiality and authenticity to the executed code and stored data, and to prove the trustworthiness of SealedGRID nodes, components and modules. Finally, the Federated Login demands trustworthiness among the participating devices/nodes, which is ensured by the remote attestation mechanism.

It is necessary to implement an Access Control Management Service to control the information within the grid. However, it is also crucial to pair this control with the continuous assessment of the network in terms of security, as to permit or deny the use of certain services in case of risk. This is enabled by **context-awareness mechanisms**, which retrieve data about the production chain in real time (e.g., network events, alarms, raw traffic). Here we leverage Opinion Dynamics [17], a multi-agent collaborative algorithm capable of detecting attacks during their entire lifecycle, from a holistic perspective. It is designed as a framework to analyze information from external sources (e.g., IDS) together with Machine Learning techniques in a distributed way.

3 SealedGRID Components

In this section, we analyze the SealedGRID architecture focusing the SG different components: SMs, Aggregators, Utility, as well as the different technologies that each component encompasses (see Fig. 1). Moreover, the fundamental SG operations are briefly elaborated, depicting how the set of requirements discussed in the previous sections are met.

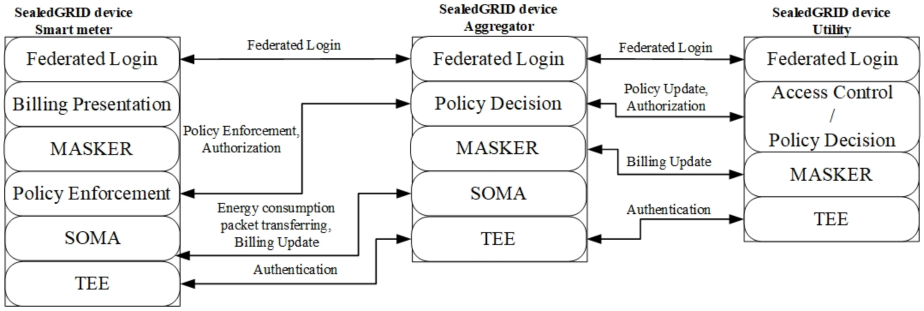

Fig. 1. Architectural components and integrated modules for SealedGRID

The SealedGRID SM communicates with other components without extra authentication using the Federated Login module. Also, it deploys the SOMA module, which includes: a) the SOMA client to request to join in a domain and become part of the SOMA network, and b) the SOMA authenticator used by an already authenticated SM in a SOMA network to handle a new join request; its certificate is issued by the domains CA and stored within the TEE. Moreover, it generates the energy consumption readings and constructs the related packet within the MASKER where the TEE is involved. After its construction, it is forwarded to a SealedGRID Aggregator. Also, it receives periodical reports with billing updates through the MASKER. Finally, it plays the role of a PIP and PEP. The PIP determines the severity degree of the area, which can be requested by the PDP placed in the intermediate nodes of that domain. The PEP's role is utilized to access data or request the control of another SealedGRID SM from the same or different domains.

The SealedGRID Aggregator authenticates and authorizes new devices in a domain (using SOMA) and aggregates individual readings without being able to infer private information from these messages (using MASKER). As explained before, the security of these operations is ensured by the TEE. As for the authorization, it plays the role of the PEP, since it is responsible for policy enforcement in its domain, according to the policy defined by the Utility. Therefore, it is also considered as an intermediate level PDP, taking access control decisions in a local level.

The SealedGRID Utility is responsible to maintain DR and to calculate the billing by computing the total consumption of customers at the end of the billing period (for which MASKER is leveraged). Moreover, it is liable for issuing the systems policy, integrating the Federated Login module to provide seamless communication between SealedGRID components from different domains. Finally, a Utility plays the role of the PDP role to issue the system access control policy. However, it is also considered as an individual PEP, since it should ensure the enforcement of the security policy in its domain.

4 Discussion and Future Work

This section briefly outlines the fundamental operational and security requirements (i.e., service, infrastructure, and customers) that SealedGRID satisfies.

Service Requirements: Energy distribution services, require availability and accuracy in DR. SealedGRID utilizes the SOMA module to ensure availability, which creates a mesh network for providing authentication and trust management, avoiding single points of failure. Moreover, it employs the MASKER module to inform the Utility about the aggregated energy consumption in real-time, limiting the imposed overheads to the Utility.

Infrastructure Requirements:The SG infrastructure requires a scalable network as the number of customers' varies, while its components should interoperate and communicate to each other for seamless energy distribution. To ensure it, system's monitoring is required for detection of abnormal operation. Moreover, the issuance and enforcement of a system policy guarantees the appropriate system operation. The SOMA module provides scalability regardless of the number of involved components and the frequency of components join and leave. The Federated Login module grants unstoppable communication to the participated components without repetitive identification/auhtentication. In addition, Context Awareness Manager module monitors the system behavior based on information from real time events. Finally, SealedGRID sets the role of PDP in the Utilities to issue the system policy and the PEP's role in Aggregators for enforcing it in their domain, to ensure that system operations run smoothly and the participated components follow the policy.

Customer's Requirements: The SG customers require an authentication procedure to access multiple energy distribution systems with a single instance of identification. Moreover, they demand confidentiality to their personally identifiable information and stable energy supply without energy cutoffs. SealedGRID uses the SOMA module to authenticate new SMs and the Federated Login module to provide single-sign-on to access energy distribution systems by employing only one identification/authentication step within the whole SealedGRID domain. Finally, it implements the MASKER module which not only protects customers' personal data utilizing a TEE, but also enables the DR functionality for persistent and steady power supply.

Altogether, we achieve a federated, dynamic and secure SG architecture where the access control to critical resources, trust and privacy are considered. As future work, we intent to implement the proposed architecture in order to show the feasibility of the security components for practical use cases based on federated, complex and heterogeneous Smart Grid environments.

Acknowledgement This work was supported by the European Commission under the SealedGRID project (H2020-MSCA-RISE-2017) with GA no. 777996.

References

1. Mohammadali et. al. A novel identity-based key establishment method for advanced metering infrastructure in smart grid. *IEEE Transactions on Smart Grid*, 9(4):2834–2842, July 2018.
2. *Trusted Computing Group, TPM Mobile with Trusted Execution Environment for Comprehensive Mobile Device Security, Whitepaper, June 2012.*
3. *GlobalPlatform: Trusted Execution Environment System Architecture, 2011.*
4. *CEN/CENELEC/ETSI, Smart Grid Information Security, December 2014.*
5. F. Knirsch et. al. Error-resilient masking approaches for privacy preserving data aggregation. *IEEE Transactions on Smart Grid*, 9(4):3351–3361, July 2018.
6. *DNP3 Users Group Technical Committee. DNP3 Secure Authentication Specification Version 2.0, DNP Users Group Documentation as a supplement to Volume 2 of DNP3. Technical report, DNP Users Group, 2008.*
7. *IEC TS 62351 series, Power systems management and associated information exchange Data and communications security, Tech specification, 2007.*
8. W. Chin et. al. A framework of machine-to-machine authentication in smart grid: A two-layer approach. *IEEE Communications Magazine*, 54(12):102–107, December 2016.
9. R. Lu et. al. Eath: An efficient aggregate authentication protocol for smart grid communications. In *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1819–1824, April 2013.
10. Alcaraz, cristina and javier lopez. ”secure interoperability in cyber-physical systems.” security solutions and applied cryptography in smart grid communications. igi global, 2017. 137-158. web. 19 apr. 2019. doi:10.4018/978-1-5225-1829-7.ch008.
11. *Veichtlbauer et. al Advanced metering and data access infrastructures in smart grid environments. In: The seventh international conference on sensor technologies and applications (SENSORCOMM), p. 638, 2013.*
12. Cristina Alcaraz et. al. Policy enforcement system for secure interoperable control in distributed smart grid systems. *Journal of Network and Computer Applications*, 59:301 – 314, 2016.
13. *Killing the Password and Preserving Privacy with Device-Centric and Attribute-based Authentication*. Zenodo, February 2019. https://arxiv.org/abs/1811.08360.
14. Demertzis et. al. Self-organised key management for the smart grid. In Symeon Papavassiliou and Stefan Ruehrup, editors, *Ad-hoc, Mobile, and Wireless Networks*, pages 303–316, Cham, 2015. Springer International Publishing.
15. Georgios Karopoulos et. al. Masker: Masking for privacy-preserving aggregation in the smart grid ecosystem. *Computers Security*, 73:307 – 325, 2018.
16. Karopoulos et. al. Towards trusted metering in the smart grid. In *2017 IEEE 22nd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pages 1–5, June 2017.
17. Rubio et. al. Tracking advanced persistent threats in critical infrastructures through opinion dynamics. In *Computer Security*, pages 555–574, Cham, 2018. Springer International Publishing.