Towards Applied Security-by-Design for DER Units

A. Veichtlbauer[*], O. Langthaler[§], D. Engel[*]
[*]Josef Ressel Center for User-Centric
Smart Grid Privacy, Security and Control
[*,§]Salzburg University of Applied Sciences
Puch/Salzburg, Austria
{oliver.langthaler, armin.veichtlbauer, dominik.engel}@fh-salzburg.ac.at

C. Kasberger
SE Product Line Software &
Internet Services
Fronius International GmbH
Thalheim/Wels, Austria
kasberger.christian@fronius.com

F. Pröstl Andrén, T. Strasser
Electric Energy Systems
Energy Department
AIT Austrian Inst. of Technology
Vienna, Austria
{filip.proestl-andren, thomas.strasser}@ait.ac.at

***Abstract*—For upcoming smart grid information and communication architectures, security is an indispensable requirement in order to ensure security of supply, to prevent damages to the electricity supply, loss or manipulation of personal or accounting information, etc. This must be taken into account throughout all developmental phases when creating such a framework, i.e., from the design phase on. Therefore, a Security-by-Design (SbD) approach has to be used which is able to address all potential harms to the envisioned system. Especially through the integration of distributed energy resources, new stakeholders (who may have low awareness of potential security risks) have to be considered, e.g., private households with photovoltaic/battery systems. Through the usage of the Internet for the exchange of sensitive data, intrusions from malicious attackers are facilitated. To cope with this, distributed energy resources have to include a comprehensive security subsystem. In this paper, an exemplary solution for the consideration of these issues in highly distributed infrastructures is given.**

I. Introduction

Recent developments in the domain of Information and Communication Technology (ICT) help to turn the operation of power systems into an intelligent automation and control infrastructure, a "Smart Grid" [1]. This kind of "smartness" is necessary in order to cope with future needs [2]. For instance, in order to integrate Distributed Energy Resources (DER) on a large scale, it has to be possible to exchange monitoring and control data between DER components and utility supervisory control systems. An unavailable or insecure ICT infrastructure could potentially cause instabilities, which might in extreme cases lead to outages of the power supply. Consequently, smart grid security has been deemed important [3], [4].

Today, DER units are often controlled via dedicated network infrastructure with utility supervisory control systems; also, the usage of open communication systems such as the Internet for smart metering becomes common. This may lead to substantial difficulties if non-authorized entities are able to access or even manipulate data without being recognized immediately [5]. As the physical infrastructure of public communication networks has to be taken as it is, countermeasures to potential threats have to be located mainly at the end devices. Thus, the main aim of this work is to define a kind of middleware at the involved end devices (i.e., DER units), which is able to protect against these threats. For doing so, security issues have to be integrated early on, thus constituting an SbD approach.

978-1-5090-1314-2/16/$31.00 © 2016 IEEE

II. Related Work

DER (especially Photovoltaic systems) are nowadays reaching or already exceeding the hosting capacity of the power grids in a number of regions and countries (e.g., Germany or Italy) [6]. This creates additional operational challenges for energy utilities, mostly due to the large numbers of DER components, their variable power output and through their uncoordinated response to changing conditions in the power grid. The smart grid approach is one of the most promising solutions to use the existing grid infrastructure in a more efficient way, thus allowing higher penetration levels of DER [1]. To capture the benefits of intelligent power grids, it will be necessary to develop DER components with smart functions (remote control, monitoring, ancillary services, parametrization, etc.). This opens the ability to effectively manage the large numbers of DER units and to utilize their "smart" capabilities. Distributed automation and thus an appropriate ICT infrastructure play key roles to implement such a coordinated system approach [6].

In order to realize such ICT infrastructures, in many cases public networks such as the Internet are used as a basis for forming an Internet of Energy [7], [8]. Consequently, security has become a major issue which has to be addressed thoroughly. In the area of home automation, OSGi-based several frameworks (e.g., OGEMA, OpenMuc, IoTSys, and OpenHAB) have been realized which integrate security issues to some extent [9]. However, basic features such as end-to-end encryption are not necessarily supported. For the smart grid itself, there are several overview publications listing general security challenges and requirements [4], [10]. The CEN-CENELEC-ETSI Smart Grid Coordination Group (SGCG) supports standardization and awareness with its Smart Grid Information Security white paper [11]. For the field of smart metering, also some standardization activities exist [12].

There are plenty of publications about some theoretical aspects of smart grid security; e.g., regarding communication security, a combined approach of end-to-end and hop-by-hop security is provided by [13]. A public key infrastructure is proposed by [14]. [15] provides an architecture for a secure metering infrastructure. [16] discusses model based approaches for systems engineering with respect to smart grid security. Also, there are some papers (e.g., [5]) about relevant attacks against DER units.

However, these contributions are rather focusing on the description and analysis, than giving concrete hints about how these attacks could be mitigated in practice. The paper at hand thus tries to provide a flexible solution able to perform several mitigation activities. Hereby, the security aspect has been essential when defining the architecture, as described in the next section. The paper reflects research results which have been obtained in the "OpenNES" research project.

III. OpenNES DER Framework Architecture

In OpenNES, an open and interoperable ICT solution for the integration of renewable energy sources into smart grids is developed. It supports remote programmable DER functions, a generic communication infrastructure as well as a corresponding application modeling method for DER applications. An important focus of the project is related to the specification of an access management framework for DER units, taking into account different users and roles (plant owner, plant operator, energy utility, aggregator, etc.).

Fig. 1 provides a brief overview of the basic project idea with the proposed open ICT solution supporting interoperability and scalability of future smart grid solutions, including a high penetration of DER. An important part of the project is the development and specification of the software architecture containing the following three main parts: *(i)* the "SmartOS" middleware including basic DER functionality as well as security and communication subsystems, *(ii)* pluggable software components, and *(iii)* an engineering part used for programming and configuration.

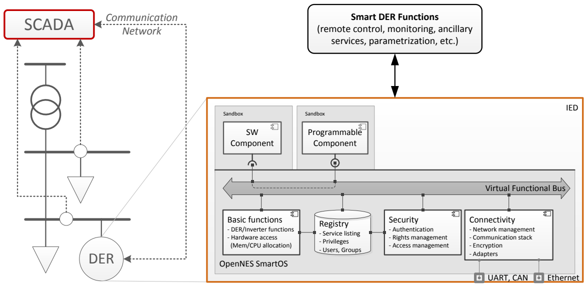

Fig. 1. Proposed OpenNES DER Framework Architecture.

The SmartOS is not a traditional operating system in the sense of Linux or Windows, but rather a hardware abstraction layer with additional functionality for handling software components and the interaction between these components. It includes common aspects like communication, security, and basic DER functions. For the interaction, a "Virtual Functional Bus" (VFB) based on the AUTOSAR concept [17] was introduced. The VFB is an integration approach comparable to the idea of the Enterprise Service Bus (ESB), but specifically developed for embedded control applications.

The software components are pluggable modules which can be removed or added in a flexible manner. They may either be developed and delivered by the DER manufacturer or by an external certified partner (e.g., a DER plant operator). They may be programmable using an external engineering environment (e.g., based on IEC 61131-3 or IEC 61499). Software components may also provide and request services from other components. This interaction is mandatory led through the VFB; this again uses the Security submodule (cf. Fig. 1) to check the legitimacy of the interaction. The OpenNES approach integrates SbD in a twofold manner:

- First, a list of general security threats (which have been identified as relevant to the proposed infrastructure) are natively addressed by respective countermeasures. However, this list does not claim completeness, as in security engineering the possibility of an emergence of a new threat always needs to be considered. If such a threat exploits previously unknown vulnerabilities, i.e., it is not sufficiently covered by countermeasures to previously known threats, it has to be added to the list of attacks.
- Thus, as a second measure, the SbD approach has to support an according extension of countermeasures. This covers the alteration of existing security features, but also the integration of additional security functionality in order to respond to the new threat. This may be achieved in several ways, e.g., by updating the software of an "Intelligent Electronic Device" (IED). If these updates are to be installed remotely, the update process also has to be secured with the latest known security technologies in order to prevent manipulation.

IV. Security Threats

The above introduced SmartOS allows for a plethora of new applications in the energy field; especially distributed control, which is a precondition for integrating DER units into smart grid systems. As a downside, an open ICT environment is also exposed to unintended usage. This includes, but is not limited to, deliberate acts which are able to manipulate technical systems in a harmful way. The German "IT Grundschutz" Catalogue [18] further lists force majeure, organizational shortcomings, human error, and technical failures as threat sources. However, in this work, the focus had been set on deliberate acts, i.e., external attack scenarios of human origin. Potentially, also natural disasters might be an issue; yet these scenarios are already considered in current grid solutions [19].

From current security publications, e.g., [3], an overview of potential attack scenarios can be derived. These attacks have to be screened regarding their relevance to smart grid environments. Again, the result of that is a current snapshot; thus the envisaged solution has to be flexible enough to react to the appearance of threats which are not already listed (e.g., a Stuxnet-like virus specifically designed to sabotage power systems might constitute such a new threat occurrence). For now, the following overview of relevant generic attack scenarios has been identified:

- *Man-in-the-Middle attacks:* Session hijacking (gaining unauthorized access by taking over a valid session) or spoofing (forging network addresses in order to impersonate another system or to remain anonymous) may be used to manipulate accounting data or – even worse – control data. Wiretapping (monitoring and/or recording of network traffic) may be used to disclose private data, but also to collect unencrypted access data.

- *Other network based attacks:* Password guessing (attempting to gain access to a system by systematically and exhaustively trying possible passwords) may be used to gather access to critical systems, port scanning (systematic identification of available services on a host) may be used as preparation of a more specific attack, and DoS (Denial-of-Service, i.e., flooding a host or network resource with invalid requests) may be used in order to render a service or resource (e.g., a DER remote control function) unavailable to its intended users.
- *Attacks on/via software components:* Programming overflows (attempting to go beyond the boundaries of allocated memory) may be used to produce errors and/or to gain access to restricted memory areas and can thus be used to disclose private data or – even worse – to insert malicious code into critical control functions.

Threats may lead to unintended behavior of the technical system under consideration. As for the ISO/IEC-27000 standard series for information security [20], the basic information security attributes are: *(i)* Confidentiality, *(ii)* Integrity, and *(iii)* Availability denoted as CIA. In [21], availability is defined as delivery of a service to a user with appropriate rights. In analogy, confidentiality is defined as non-delivery of a service to a non-user, i.e., someone lacking the rights to access the service. Finally, integrity is interpreted as the situation where a technical system has not been manipulated by outside threat sources. For ICT systems used in the smart grid domain, system vulnerabilities which are exploited by the above listed threats might cause harm to all three security attributes:

- *Confidentiality:* In smart grid architectures, distributed control data has to be transported. This includes sensor data from smart meters or other relevant data sources, e.g., Phasor Measurement Units (PMUs), but also actuator data such as characteristic curves for inverter-based DER or storage devices. As a consequence, only necessary data should be transmitted, and the use of appropriate encryption techniques is strongly advised.
- *Availability:* The ICT infrastructure is used to transport control signals (for DER, substations, etc.). Thus, the non-availability of this communication subsystem (e.g., due to a DoS attack) might lead to dysfunction of such a distributed control system. Although the electrical systems are typically designed to allow for local control functionality, a longer lasting outage of communication components may cause severe harm to power systems.
- *Integrity:* The most severe danger to smart grid systems is violation of the control logic's integrity. As a result, the system's reaction to sensor inputs does not follow the established rules, but may cause irrational or even dangerous actuator settings. The manipulation may not immediately be recognized, yet the system's behavior may already be abnormal. In extreme cases, this may even be harmful to its environment.

V. Countermeasure and Mitigation Design

As a consequence of the aforementioned considerations, an ICT subsystem of a smart grid solution has to be hardened against these potential threats, i.e., the vulnerabilities to threats (especially deliberate acts) have to be minimized. Therefor, some appropriate countermeasures have to be instated. These security countermeasures have been incorporated into the design of the OpenNES SmartOS in a number of ways:

- *Controlled IED ecosystem:* An ecosystem is enforced on all OpenNES IEDs, which by default requires that all software components and all updates of applications are signed by their manufacturers. Furthermore, all applications are running in sandboxes with their external access being limited to API (Application Programming Interface) calls.
- *Encryption:* Encryption of all transmitted data is performed by a dedicated Connectivity sub-module which handles all in- and outbound traffic, using a Public Key Infrastructure (PKI) and public or private trust centers. Furthermore, all stored data has to be encrypted to avoid bypasses of the SmartOS security.
- *Role-Based Access Control (RBAC):* Throughout the entire OpenNES system, RBAC is strictly enforced. By way of the Security sub-module, for all reading or writing access attempts, the user rights to the respective resource are checked. Also, all communication activities to other components (be it within the IED or between different IEDs) require authentication and authorization. Information about users, groups, and their respective privileges are stored in a registry database.
- *Additional measures:* Firewalls and intrusion detection systems are placed at all strategically necessary locations. Finally, dedicated networks are used whereever available.

The RBAC approach is the core concept of the OpenNES security architecture. It consists of a compilation of generic use cases, whose relationships are illustrated in Fig. 2. They include elemental tasks such as the process of authenticating at a target system (e.g., an IED), accessing a resource on a system (e.g., taking readings), performing maintenance tasks on a device (e.g., changing settings) and, above all, managing access rights.

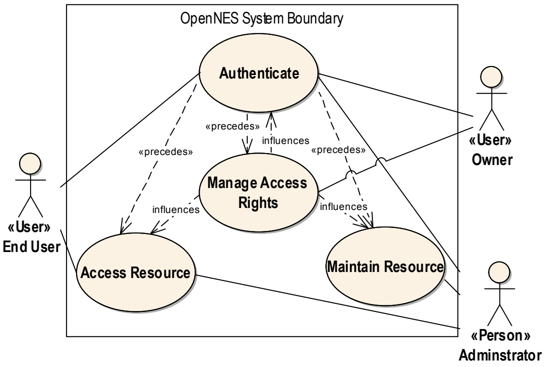

Fig. 2. Communication Use Case Diagram.

In Fig. 3, the allocation of access rights to a user by an administrative instance (i.e., the "owner" of a system or system component), is shown in detail. For all subsequent activities, the presence of appropriate access rights is required. This applies to applications demanding these forms of access as well as to persons using these applications.

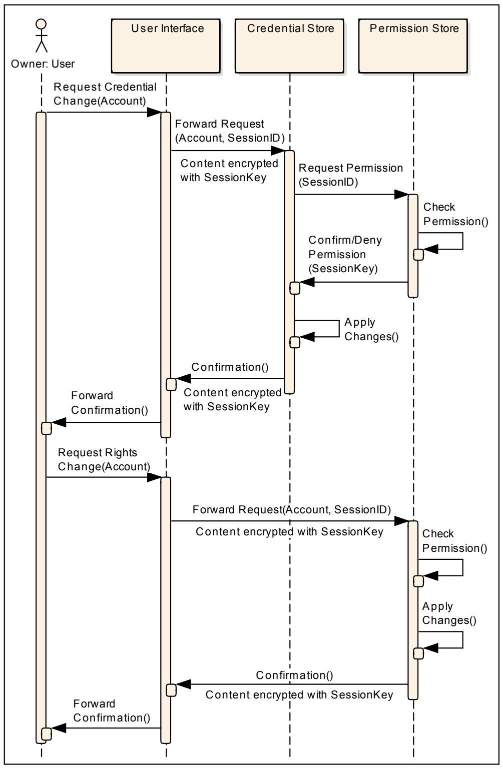
Owner: User
User Interface
Credential Store
Permission Store
Request Credential Change(Account)
Forward Request (Account, SessionID)
Content encrypted with SessionKey
Request Permission (SessionID)
Check Permission()
Confirm/Deny Permission (SessionKey)
Apply Changes()
Confirmation()
Content encrypted with SessionKey
Forward Confirmation()
Request Rights Change(Account)
Forward Request(Account, SessionID)
Content encrypted with SessionKey
Check Permission()
Apply Changes()
Confirmation()
Content encrypted with SessionKey
Forward Confirmation()

Fig. 3. Rights Management.

VI. Conclusions and Further Work

Following a discussion of recent and current ICT developments in power systems, a DER middleware architecture has been introduced in this paper incorporating a SbD concept. As part of this approach, a number of threats to this architecture have been identified and appropriate countermeasures have been gathered. It has then been shown how these countermeasures have been incorporated into the OpenNES architecture. In order to be flexible to react to future developments, the architecture also allows for later integration of further countermeasures if needed and available.

With such an architecture, implementations can now be realized, and appropriate testbeds can be set up. With this prototype, the effectiveness of the proposed SbD approach can be validated, but also the correctness of the implementation can be tested. Appropriate test results provided, the architecture at hand will serve as basis for our research group's further R&D activities. One future activity may be to pursue an independent security audit or a certification of the proposed solution. Also, a broader adoption in the smart grid domain (beyond DER) seems to be desirable. From an academic perspective, the link to current smart grid privacy discussions may be fruitful.

Acknowledgment

This work is funded by the Austrian Ministry for Transport, Innovation and Technology (bmvit) and the Austrian Research Promotion Agency (FFG) under the "ICT of the Future Programme" in the OpenNES project (FFG No. 845632).

Also, the financial support of the Josef Ressel Center for User-Centric Smart Grid Privacy, Security and Control by the Austrian Federal Ministry of Economy, Family and Youth and the Austrian National Foundation for Research, Technology and Development is gratefully acknowledged.

References

[1] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, 2010.

[2] V. C. Gungor et al., "A Survey on Smart Grid Potential Applications and Communication Requirements," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 28–42, 2013.

[3] A. Barenghi and G. Pelosi, "Security and Privacy in Smart Grid Infrastructures," in *Internatinal Database and Expert Systems Applications (DEXA) Workshop*, 2011, pp. 102–108.

[4] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-Physical System Security for the Electric Power Grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[5] B. Kang et al., "Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations," in *2015 IEEE Conference on Emerging Technologies Factory Automation (ETFA)*, 2015, pp. 1–8.

[6] International Energy Agency (IEA), "Technology Roadmap Smart Grids," IEA Paris, France, Tech. Rep., 2011. [Online]. Available: http://www.iea.org

[7] V. C. Gungor et al., "Smart Grid Technologies: Communication Technologies and Standards," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 4, pp. 529–539, 2011.

[8] A. Q. Huang et al., "The Future Renewable Electric Energy Delivery and Management (FREEDM) System: The Energy Internet," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 133–148, 2011.

[9] M. Pichler et al., "Evaluation of OSGi-based Architectures for Customer Energy Management Systems," in *2015 IEEE International Conference on Industrial Technology (ICIT2015)*, 2015, pp. 2455–2460.

[10] E. Egozcue et al., "Smart Grid Security – Annex II. Security aspects of the smart grid," European Network and Information Security Agency (ENISA), Tech. Rep., 2012.

[11] *Smart Grid Information Security*, CEN-CENELEC-ETSI Smart Grid Coordination Group Std., 2012.

[12] *Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)*, German Federal Office for Information Security Std., Rev. 1.3, 2014.

[13] A. Bartoli et al., "Secure lossless aggregation for smart grid M2M networks," in *First IEEE International Conference on Smart Grid Communications*, 2010, pp. 333–338.

[14] A. R. Metke et al., "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, 2010.

[15] D. von Oheimb, "IT Security architecture approaches for Smart Metering and Smart Grid," *Smart Grid Security*, pp. 1–25, 2013.

[16] C. Neureiter, D. Engel, and M. Uslar, "Domain Specific and Model Based Systems Engineering in the Smart Grid as Prerequesite for Security by Design," *Electronics*, vol. 5, no. 24, pp. 1–42, 2016.

[17] M. Broy et al., "Toward a holistic and standardized automotive architecture description," *Computer*, vol. 42, no. 12, pp. 98–101, 2009.

[18] "IT-Grundschutz Catalogues: Version 2013," German Federal Office for Information Security, Tech. Rep., 2013.

[19] D. Chassin and C. Posse, "Evaluating North American electric grid reliability using the Barabási–Albert network model," *Physica A: Statistical Mechanics and its Applications*, vol. 355, no. 2, pp. 667–677, 2005.

[20] *ISO/IEC 27000:2016 Information technology – Security techniques – Information security management systems – Overview and vocabulary*, International Organization for Standardization (ISO) Std., 2016.

[21] E. Jonsson and L. Pirzadeh, "Identifying Suitable Attributes for Security and Dependability Metrication," in *7th International Conference on Emerging Security Information, Systems and Technologies (Securware 2013)*, 2013, pp. 1–7.