On Demand for Situational Awareness for Preventing Attacks on the Smart Grid

Yegor Shovgenya, Florian Skopik
AIT Austrian Institute of Technology GmbH
Vienna, Austria
yegor.shovgenya.fl@ait.ac.at
florian.skopik@ait.ac.at

Klaus Theuerkauf
ifak - Institut für Automation und Kommunikation e.V. Magdeburg
Magdeburg, Germany
klaus.theuerkauf@ifak.eu

***Abstract*—Renewable energy sources and widespread small-scale power generators change the structure of the power grid, where actual power consumers also temporarily become suppliers. Smart grids require continuous management of complex operations through utility providers, which leads to increasing interconnections and usage of ICT-enabled industrial control systems. Yet, often insufficiently implemented security mechanisms and the lack of appropriate monitoring solutions will make the smart grid vulnerable to malicious manipulations that may possibly result in severe power outages. Having a thorough understanding about the operational characteristics of smart grids, supported by clearly defined policies and processes, will be essential to establishing situational awareness, and thus, the first step for ensuring security and safety of the power supply.**

Keywords—smart grid; situational awareness; smart generator; industrial control systems.

I. Introduction

Until this decade, the power generation was concentrated in a few locations, i.e. "classic" power plants, and the energy output was highly predictable, which allowed planning reliable measures for adapting generation to higher or lower consumption. However, the European power grid has been changing significantly with the increasing integration of renewable energy sources. This is particularly challenging, since renewable sources, such as solar and wind power offer rather unpredictable amounts of energy over time. Though, the power generation and consumption in the grid need to be held constantly in balance.

The integration of distributed renewable energy sources has different pace across Europe and proceeds particularly fast where the initiative to install a power generator is financially encouraged (as in Germany), or where the weather conditions make renewable energy sources most profitable (as solar energy in Italy and Spain). In Germany, for instance, photovoltaics generates up to 50% [3] of overall power under optimal weather conditions. This challenges the grid operators, who have to provide flexible mechanisms of balancing consumption and production.

A. Problem statement

To manage the distributed power generation in the grid, its operators mostly have the technical means to remotely control small-scale individual generators and photovoltaics inverters. This remote control functionality may be a mandatory condition under which small-scale energy producers can sell a certain amount of produced power to the grid (as it is in Germany [3]).

In this paper we discuss a scenario where the means of managing the grid are consciously misused by an adversary. We further propose some measures countering such attacks.

B. Paper Outline

The remainder of this paper is outlined as follows. In Section II we describe future conditions that will make smart grids vulnerable and give a brief overview of some studies relevant to the topic. Section III illustrates the attacker's possible course of action, and Section IV comprises the steps that could prevent probable attacks. Section V concludes the paper.

II. Background and related work

Due to the complexity of the generation landscape, grid operation concepts came up, which are mostly driven by smaller regional energy suppliers. These concepts are also consolidated into the notion of a "smart grid". Smart grids are characterized [9, p. 33] by:

- Comprehensive communication infrastructure
- Local generation as well as traditional generation
- Storages (in chemical, potential, physical energy form)
- Virtual power plants as connection from generation-storage-consumption in a region
- Dynamic load management and dynamic pricing of electrical energy
- Stochastic effects in generation planning and operation because of renewable sources.

To realize these changes, a strong interconnection of devices involved in the grid operation is required. The fast innovations in computing have led to more intelligent electrical equipment in the field. While the first microcontroller-equipped devices were designed to implement more complex control algorithms, current devices use IT technologies to implement communication interfaces. The process of IT-technologies integration is usually iterative and driven by functionality, usability and safety rather than security.

The implementation of smart grid concepts, such as the virtual power plant (numerous small generators acting as a unified market player) requires extensive communication to

achieve the targets of low pricing, local generation and consumption.

With generation in multi-directional networks the over-current protection (e.g. as a result of a lightning strike) must also be distributed to detect and prevent islanding of network parts that are incapable to control their frequency and phases. Once dispatched, these parts will take time to reintegrate into the network. This negative effect could be avoided, if a distributed control logic prevented the part from disconnecting.

In conclusion, distributed control of equipment is needed to fulfill the common goals and challenges of smart grid operations. But the communication and security standardization were not considered in the past. This led to vulnerabilities that impose threats to the electric grid as a critical infrastructure.

The future grid on the low voltage level will consist of the following communicating elements:

- Smart meters for consumption measurement
- Inverters or small transformer stations for power generation sensing and control
- Interconnected protection devices
- Load management devices in private consumer space (electric car charging, switching of washing machines)
- Gateways to existing grid control infrastructures.

Smart meters will communicate with the control center of a respective grid operator via data concentrators, that gather power consumption readings from meters and send aggregated readings to the control center one to several times per day.

Consumers, including private households, will adjust their power use according to the actual tariff they receive from their provider several times a day. Such an adjustment is performed automatically by the electrical appliances that receive current tariff information from a dedicated device[1] connected to the energy provider's control center.

Due to very large numbers in which smart meters will have to be deployed, strict constraints arise for the price of the individual device. There are reports [2] revealing that at least first versions of hard- and software for smart grid devices did not use state-of-the-art encryption, and were susceptible to cryptographic attacks. Even on some industrial control systems (ICS) components with high market penetration, administrator passwords are reported to be hardcoded into the firmware [15].

Existing load management solutions such as *Funkrundsteuertechnik* (long wave control) in Germany or *radio teleswitching* in the UK were crafted under functional requirements two decades ago. At least the *Funkrundsteuertechnik* does not cover security aspects [10].

A 2011 study [12] provides a good overview of major incidents involving SCADA systems since 2003. It also reveals at least 7489 ICS systems across the world that were accessible from the Internet with the help of the publicly available Shodan search engine. Another research from 2013 detected that "half a million ICS and SCADA devices are exposed in public databases, at risk of attack" [13]. The state-of-the-art of ICS security is further illustrated by a white paper [4] stating that 54% of all European ICS that are accessible through the Internet are also exposed to remote attacks.

[1] Example is available at: http://www.efr.de/produkte/efr-smart-grid-hub/#/GPRS

III. Course of Attack on a Smart Grid

The attacker of this use case represents a well-funded organization, having expert-level knowledge in software development, mechanical and electrical engineering and cryptography. The attacker's goal lies in shutting down segments of the energy grid at the scale involving at least tens of thousands of customers, the motivation being either political (spreading chaos and provoking the population), or financial (harming a market opponent's reputation or damaging their equipment).

A. *Phase 1: Attacking the grid control center*

To acquire privileges of the grid operator under conditions described in Section II, the attacker can take the following steps:

1. Obtain technical documentation on targeted smart meters, communication channels and protocols used.
2. Obtain physical access to smart meters. Conduct reverse engineering of available smart meters or test them for vulnerabilities known to the attacker, for example as described in [1].
3. Connect to the communication medium (e.g. Power Line Communication or wireless network) between a functioning smart meter and its data concentrator.
4. Decrypt signals sent by smart meters by sniffing their communication with a data concentrator.
5. Simulate a smart meter to a data concentrator, using the protocol details and credentials obtained from reverse engineering or signal sniffing. Send malicious signals to the concentrator.
6. Establish a foothold in the concentrator: execute malicious code on it, obtain limited or full control over the concentrator.
7. Begin communicating with the grid control center on behalf of the concentrator, or inject malicious input into their communication.
8. Run or plant malicious software on the control center server, possibly obtain limited or full control over it using known vulnerabilities.

B. *Phase 2: Attacking smart power generators*

After the attacker has infiltrated the grid operator's control center, s/he uses the center's capacities to damage the grid and bring it to a blackout.

The attacker could have also taken over the control center in another way than described in Phase 1; essential is that he is able to issue commands to the infrastructure in the same way the legitimate grid operator is able to.

This second sequence of the adversary's actions is as follows.

1. Obtain documentation on smart grid structure and power lines architecture in the targeted regions. The source may be a third-party, an accomplice among the

grid operator's employees, or resources available from the control center, where the attacker already established a foothold.

2. Engineer a tariff update message that sets a very low price for received power.
3. Distribute the fake tariff among consumer tariff management devices. During the first two hours after receiving the malicious update, consumers start perceiving the current energy prices as very low.
4. Using the provider control center's resources, the attacker commands all available small-scale energy generators to stop feeding power to the grid.

Because of the generally low price for renewable energy on the European Energy Exchange (EEX) the energy supplying organizations will buy mostly renewable energy in form of solar and wind and will reduce their traditional power plants.

After step 3 the enterprise and private customers in the targeted grid segments perceive their current power tariff as very cheap. To utilize these low prices, they increase their consumption to the best available extent.

To make his attack more effective and demoralizing, the adversary may be active in several European countries simultaneously. Here we consider Germany, Italy and Spain as possible objectives. Germany, as mentioned before, relies particularly on solar power; Italy also has the need to import power due to a shortage of own power generation.

If the attack was launched on a hot, sunny but not windy summer day in Europe, the power request in Germany, and especially Spain and Italy will be high due to the use of air conditioning systems. Low suggested prices will further enhance the power consumption, as mentioned above.

The situation now can be described as:

- high demand stimulated by false sensor information;
- high amount of solar power in the system.

The latter condition can be monitored by the attacker using modern IT services[2].

After step 4, a large number of solar power plants might get disconnected. Especially in areas where the power grid is weak, the grid operator will try to control the great power demand by using the typical primary (active within milliseconds) / secondary (seconds) and tertiary (minutes) control mechanisms, as disconnection of great loads or use of fast reacting storage facilities.

If the lost generation power in this grid segment is bigger than the primary to tertiary control backing, the grid frequency in the grid segment will drop, and the segment will require power from other grid segments, which will stress the power transfer lines.

In case this discrepancy between energy demand and supply is too large and persists over a longer time frame, power grids in the targeted regions will exceed either the transfer line capacities or the remaining generation power, so that generation facilities will be shut down. The affected grid segment may then face a local blackout, as it happened in the USA in 2003 [11] and in Germany in 2006 [14].

If multiple European countries will be targeted at the same time, a cascading propagation of power outage across Europe is possible.

After several neighboring grid segments are switched off, the grid reconstruction will take time, because no phase and frequency information can be obtained from the perimeter segments. The reconstruction in this case will be done by bottom up strategy which integrates load and generation capacities over several iterations.

IV. Proposed Security Measures

A. *Situational awareness in the grid*

The attack described in Section III makes use of insufficient protection of field devices and, more importantly, the fact that the grid provider is not informed about the operational situation, nor about security-relevant events in the low-voltage grid (such as the reception of unexpected requests on a data concentrator). The solution here is what the US Committee on National Security Systems defines as *situational awareness* [16, p.69]: "Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future."

Today, industrial components and technologies often lack a complex approach to security and situational awareness, as outlined in Section II. This may have serious implications even without malicious intrusion, as with the 2003 US blackout that is attributed to insufficient situational awareness [1, p.159]. A number of successful attacks targeting ICS was also observed in recent years, of which Stuxnet is probably the most prominent one.

Providing situational awareness requires effective monitoring and security of both components and workflows used in the grid. The following subsection describes these measures in more detail.

B. *Security by design of field devices and processes*

The ability to switch off large parts of the renewable energy infrastructure, as described in the attack scenario in Section III, will depend on the ability to disable the corresponding virtual power plant, or to fabricate wrong power generation data.

The central points the blackout attack will rely on are:

- sufficient network access to actuators and sensors;
- ability to remotely plant software on field devices;
- insufficient cryptography of communication, especially on field level.

Many facets of an attack could be avoided by proper design of devices and processes. To address these issues, we consider the following steps necessary.

First, while measurement of generation parameters such as voltage, set-point, power-factor, phase and frequency has to be continuous for a reliable grid operation, the capability to lower or switch off power generation or consumption does not.

[2] An example is available at: http://www.eex-transparency.com/

Therefore, actuators and sensors (mostly smart meters) should have separate network connections and controllers. Hereby actuators should only be active on demand and receive commands e.g. via SMS over GSM or long wave transmission. The connection should be deactivated after predefined packet/byte counts. Every access must trigger a message to a predefined communication instance that can only be changed through hardware access to devices. Each actuator event must be authorized by a Transaction authentication number (TAN) that will hinder replay attacks. Working fallback measures must be designed, in case TAN-lists run empty.

Second, the use of real time clocks must be restricted to write-only data storages. After obtaining access to devices in the grid, the attacker may plant software that will execute a predefined sequence of commands at certain points of time, without being triggered by the attacker.

Therefore real time clocks on field devices should only offer local and not remote readout. Software-based time measurement must be prevented on both actuator side (by enabling the actuator controllers on demand only) and sensor side (by watchdog resets). Messages with sensor information will be time-stamped when arriving at the storage or in the grid-operator's SCADA system.

Third, the messaging services in the grid must be robust and secure by design. In particular:

- No unencrypted or, in case of short message service, unauthenticated service must be offered.
- Encryption algorithms and parameters must correspond to the state-of-the-art and use salts.
- Credentials must be changed regularly, and not only in rare cases or emergencies.

The latter notice also applies to any credentials used within the smart grid. A reliable algorithm for credentials distribution and revocation must be developed or chosen, specifically for use by network operators.

The grid manipulation described in Section III could be avoided if control actions required two-factor authorization where:

- redundant messages from different actors are needed for changing system parameters;
- multiple communication channels must be used (e.g. long wave control, GPRS, optic fiber etc.).

V. Conclusion

The imminent advance of smart grids in Europe demands reconsidering established paradigms in the power supply. Infrastructures that were earlier designed for high reliability and safety must now also provide security; otherwise the highly interdependent power grid of the future will be vulnerable to serious attacks that were not possible before. Such attacks may be carried out remotely on the future smart grid using its compromised components, and will result in power outages in targeted regions.

Security of the smart grid will require:

- situational awareness of the grid operators, achieved through monitoring devices deployed across the grid;
- resilient and protected control mechanisms and processes, involving redundant communication channels and multi-factor authorization;
- a thorough design of field devices that provides appropriate access management and encrypted communication.

These concepts, together with the collaborative threat detection, incident mitigation and early warning frameworks, are currently developed within the ECOSSIAN research project.

Acknowledgments

This work was partly founded by the European Union FP7 project ECOSSIAN (607577).

For reviewing the paper and for valuable comments we also thank Roman Bolgaryn (ee13m013@technikum-wien.at) from the University of Applied Sciences Technikum Wien.

References

[1] Dantas H., Erkin Z., Doerr C., Hallie R., van der Bij G.: "eFuzz: A Fuzzer for DLMS/COSEM Electricity Meters". Delft university of technology.

[2] Smart meter crypto flaw worse than thought. Root Labs blog entry accessed at: http://rdist.root.org/2010/01/11/smart-meter-crypto-flaw-worse-than-thought/"http://rdist.root.org/2010/01/11/smart-meter-crypto-flaw-worse-than-thought/

[3] Wirth H.: Recent facts about photovoltaics in Germany. Fraunhofer ISE, 2015. Accessed at: http://www.ise.fraunhofer.de/en/publications/veroeffentlichungen-pdf-dateien-en/studien-und-konzeptpapiere/recent-facts-about-photovoltaics-in-germany.pdf

[4] SCADA Safety in Numbers. Positive Technologies. Accessed at: http://www.ptsecurity.com/upload/ptcom/SCADA_WP_A4.ENG.0018.01.DEC.29.pdf

[5] SCADA Security hardening guide. Positive Technologies: http://www.slideshare.net/qqlan/positive-technologies-wincc-security-hardening-guide

[6] Krebs R.: Increasing amount of DGs demands for continuous protection system audits and new protection schemes. Lecture notes, Siemens AG, 2012.

[7] Styczynski Z.A.: Grundlagen der Energietechnik, LENA, Otto-von-Guericke Universität, Magdeburg 2014

[8] Hannes Woiton: Netzwiederaufbau & IKT, Tennet AG 2014. Accessed at: http://www.dena.de/fileadmin/user_upload/Veranstaltungen/2014/27.11._IT-sicherheit/07_Woiton.pdf

[9] SGCG/M490/G_Smart Grid Set of Standards (SGCG/M490/G – version 3.1). CEN-CENELEC-ETSI Smart Grid Coordination Group, October 2014.

[10] Schneider M.: Sicherheit in der Rundsteuertechnik. 13. Deutscher Sicherheitskongress.

[11] Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. U.S.-Canada Power System Outage Task Force, 2014.

[12] Leverett, E.: Quantitatively Assessing and Visualising Industrial System Attack Surfaces. University of Cambridge, 2011.

[13] Ongaro F., Pericoli G.: Scada Exposure. ISGroup, 2013 (online). Accessed at: http://scadaexposure.com/report/2013-11#summary

[14] System Disturbance on 4 November 2006. Final report. Union for co-ordination of transmission of electricity.

[15] Too smart in da Cloud ++. Presentation by SCADA Strangelove Group. Accessed at: http://scadastrangelove.blogspot.co.at/2014/12/31c3-too-smart-grid-in-da-cloud.htm

[16] CNSS Instruction No. 4009: National Information Assurance Glossary. US committee on National Security Systems, 2010. Accessed at: http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf