Security Principles of Smart Grid Networks

F. Holik and J. Horalek

University of Pardubice, Faculty of Electrical Engineering and Informatics, Pardubice, Czech Republic.

filip.holik@student.upce.cz

***Abstract*—Increased power consumption and power supply variability require implementation of modern tools for intelligent management and control of grid networks. One of the most promising advancements in technology is the Smart Grid network. Unfortunately, this technology is still rapidly evolving and at this point contains many security issues. As recent attacks have shown, only some of these issues are known. This paper is using a systematic approach to detect these issues and to analyze all types of attacks on the Smart Grid networks. The last part of the paper proposes solution models for securing Smart Grid networks against found vulnerabilities.**

***Index Terms*—Smart Grid security; Smart Grid attacks; Risk management; Security risks.**

I. Introduction

The demand for electricity nowadays is higher than ever. In order to meet this demand, the current capacity of power plants and capacity of distribution networks are highly over provisioned. This precaution requires significant additional costs and increases the system complexity. Moreover, non-efficient monitoring of real-time power demands of households and companies is causing additional problems - the power generation and transport of electricity cannot be effectively regulated.

The Smart Grid (SG) is a concept of adding communication equipment into the traditional grid networks in order to connect consumers, distribution companies, and electricity generation companies [1]. Creating such a two-way information channel allows consumers to get information about their current power consumption and therefore brings an option to reduce their costs. On the electricity generation side, it allows these companies to regulate the power generation and trade with the electricity in real-time. Finally, it also allows the distribution companies to manage and control the distribution grid network.

The main benefits of the SG are more effective generation and distribution systems, more agile and reliable functionality, and effective utilization of "green devices" (like renewable sources and electric cars) and devices for the Internet of Things (IoT).

The transformation of traditional networks into the SG networks is utilizing modern computing tools and principles. This gives the opportunity for adding interesting benefits, but also poses new security risks.

One of the most publicized software attack was the *Stuxnet* worm, which caused damage to the Iran nuclear program in 2010 [2]. This worm aimed SCADA systems developed by Siemens and it was able to take control over programmable logic controllers (PLCs).

Similar attacks are currently massively deployed in Israel, which is investing billions of dollars into the cyber security research [3].

Attacks on distribution networks were also realized during the Ukraine conflict, where supervisory control and data acquisition (SCADA) systems were attacked by the Trojan horse *BlackEnergy*. This code caused blackout to the entire region of Ivano-Frankivsk [3].

The SG networks are not vulnerable only to the hacker attacks, but also to other security risks. In 2008, the power plant in Georgia, US was shut down after a computer software update. An engineer tried to upgrade a system for the plant's business network, but the patch reset the data on the control system, causing automatic safety systems to trigger the shut down [4].

These vulnerabilities and resulting attacks are caused by the fact, that the SG networks are a modern technology, not exposed to vulnerabilities for decades like traditional networks. Moreover, the SG networks are considered to be critical infrastructure and represent a significant strategical target. Security of these networks has to be therefore considered not only in the design phase, but also during realization and network operation phases.

II. The SG Networks and the Risk Management

A. *Components Used in the SG Networks*

Smart electricity meters are devices for measuring power consumption, voltage, and maximum power output. The device stores different events and other useful data. It can also perform additional actions like disconnecting a consumer from the distribution network, limiting the available power consumption (FUP), changing tariff group, etc. The meter contains a communication module - either a modem for the PLC network (transfer data to the concentrator), or for telecommunication networks (GPRS, 3G, 4G). The last wireless option is to use radio communication. Another option is to use a wired connection like RS-485, M-BUS, or Ethernet. These technologies are typically used in company networks.

Data concentrators act as an interface between electrical or radio networks and other network types - most commonly TCP/IP. Data concentrators are placed inside a substation due to the fact, that PLC traffic is not able to go through a transformer. A single data concentrator serves approximately 100 metering devices, but in some cases, can serve even more than 1000 of them. Communication with the server is primarily done over wired connection, or Wi-Fi, and mobile networks are used only as a backup.

Servers store and analyze data gathered from the measuring devices. Some of this data is available to the customers, while some of it is used only by energy distribution or generation employees. These employees can also change the state of the devices, and therefore prevent the network blackout, or set a different tariff group.

Information devices includes clients' PCs, smart phones, or information panels. All of these devices can inform customers about current power consumption, tariff group, and other values. The goal is to provide real-time feedback, which allows the customers to save the energy consumption and to reduce costs.

B. Communication Infrastructure of the SG Networks

Infrastructure of the SG networks is composed from blocks. There are four basic types of these blocks: HAN (home area network), NAN (neighborhood), and WAN (wide) [5].

HAN are the smallest topological entities of Smart Grid networks. They can be also called PAN (premise), or BAN (building). These networks contain smart meters and information devices, which allow customers to influence their power consumption. All the devices are using traditional communication technologies like PLC, Wi-Fi, BACnet protocol, or ZigBee. Other devices belonging to the HAN are: programmable communicating thermostat (PCT), energy management system (EMS), in-home display (IHD), and plug-in electric vehicle (PEV) [6, 7].

NAN are aggregating points for HAN and are located within a substation. The used communication interface for the aggregation is the data aggregator unit (DAU) - it forwards the data into the WAN. NAN is using the same communication technologies as HAN, but can also utilize ANSI C12 protocols, or WiMAX [6, 8].

WAN represent the same area as in the traditional networks. They connect NAN into the energetic company network, most often using Ethernet, broadband connection, or a mobile network [6].

Energy generation company network receives all the data from lower layer networks like HAN and NAN. This data is then used for the specific analysis. The network contains servers and control centers for SCADA and WAMS technologies. The communication within this network uses Ethernet technology with metallic or optical links [6].

C. The SG Threats Risk Management

Risk management is a suitable technique for identification, evaluation, and resolution of risks and security threats in the SG networks. The risk management is defined by the international standard ISO 31000 [9].

The goal of the risk management is to map risks and to describe their impacts according to the *cause-risk-impact* model. The process includes prioritization and decisions about solutions to minimize the impacts of the risks. Prevention of risks is done using precautions, and to reduce the impacts of risks, reactive actions are defined. The choice of a proper action has to always come from the risk analysis results.

The process of risk management includes five main phases:

- Risk identification
- Risk evaluation
- Risk level expression
- Identification of risk solving methods
- Risk reduction according to the selected strategy

These five phases include initial risk identification, analysis, evaluation; creation of reaction plan; monitoring; and prevention. The process also includes continuous communication and consultations.

Every decision dealing with uncertainty has to be supported by analysis, which allows identification of the most dangerous threats and the problems they can cause. To perform a proper analysis, enough information has to be gathered. With the higher number of high quality information, the level of risk and uncertainty decrease.

III. The SG Attacks

The following types of attacks were analyzed using the systematic approach to the network definition and the network relationship to the surroundings. The whole system was described as a control subsystem (Control Center) and controlled subsystem (Smart Grid Network). The system architecture is shown in Figure 1. The control subsystem contains control centers for SCADA and WAMS technologies and relevant inputs. The controlled subsystem contains a complete system of the SG network and relevant outputs.

A. Attacks on Communication Networks NAN and HAN

Communication networks in the area of HAN and NAN mostly use wireless technologies as was already mentioned. These technologies include mainly ZigBee, Wi-Fi, or WiMAX. The security issues of these technologies are described below according to [10].

Zigbee: Spoofed acknowledgment packets, Denial of Service (DoS) attack on AES-CTR, usage of the same keys on multiple ACLs, setting on a default encryption value when the electricity is lost.

Wi-Fi: Radio spectrum congestion, congestion of default gateway using ICMP packets, SSID visibility, Access Point spoofing, MAC spoofing, Man-in-the-Middle (MitM) attack.

WiMAX: Sending large amount of fake messages in order to increase end devices power consumption, jamming of the radio spectrum, no encryption of control frames, MitM attack.

B. Attacks on SCADA Systems

The SCADA systems are used for system monitoring and controlling of the entire electricity network. They are also connected to the data network which results in the following vulnerabilities: security issues of the used operating systems, wrong user policies management, wrong security policies (password requirements, account validity, etc.), no security software on the hosting server, DoS attack on the hosted server, insufficient network infrastructure security, no or wrongly configured firewall.

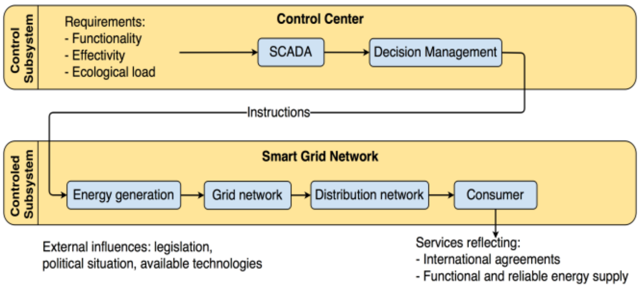

Figure 1: Smart Grid systematic approach

Moreover, the SCADA Modbus is not designed for highly security critical environments and it is therefore prone to attacks like broadcast message spoofing, direct slave control, or passive reconnaissance.

C. Attacks on AMIs

Advanced metering infrastructures (AMIs) are used within the whole SG network and they transfer a lot of data including consumers' sensitive information. AMIs are prone to the following threats: unauthorized data access and manipulation, device theft, physical damage to the device, device eavesdropping, malware infecting the device, data integrity breach, malicious device insertion - simulating a legitimate device, personnel causing data leaks.

These attacks can be further divided into the three areas: communication, physical, and system attacks.

The first part of the communication attack is to detect the used technology. After its successful detection, known vulnerabilities can be misused. GPRS, for example, can be attacked using a *femto* cell attack [11].

Another type of communication attack is connecting to the SIM in the metering device over GPRS. The purpose of this connection is to cause error state, block the modem, or fill up the SIM's memory.

Physical attacks require access to the metering device. The goal is to influence a device's functionality without causing visual damage to the device, which would be noticed by the power company employees (during the next inspection).

The first group of physical attacks uses *magnetic or electromagnetic field* in order to influence the device's ability to measure power consumption, communicate, or the ability of switching between low and high tariffication. Depending on the attack type, either a powerful magnet, or a radio transmitting jammer is used in this attack type.

A more radical type of attack uses *overvoltage*. In this type of attack, the attacker attaches a device emitting strong source of overvoltage to the proximity of the metering device. The overvoltage attack would typically permanently destroy the electronic circuits inside the device.

The last type of attack is simple *mechanical damage* to the metering device. The goal is to disable communication between the device and communication infrastructure. Example of this attack might be damage to the antenna or it's shielding; or disconnecting the PLC communicator. This type of attack includes mechanical manipulation like *phase bridging*. In this scenario, one of the phases is disconnected or bridged in order to influence the metering device's ability to measure power consumption.

In the system attack, the operating system, or configuration of the intelligent device is attacked. The operating system is usually in the form of a firmware or a lightweight-OS (when compared to the traditional operating systems).

The most common system attack is the *DoS*. The DoS uses overloading of services in order to disable communication of legitimate users. This overloading can be done by generating a large amount of requests (if the target is a server) or just packets (if the target is a network). The DoS is typically only temporal - as soon as the malicious traffic stops, the network can get back into the operational state.

The second type of attack is to *mechanically access the electric metering device* without triggering the "alarm". Triggering the alarm would immediately send the alert message to the control center. The attacker has to also try not to damage the device's security seals. If the attacker is successful, he can then block the communication channels, or access the device memory (and therefore delete the incident information).

Attacks focused on the *operating system* itself can change the behavior of the operating system; like to disable its communication abilities. The examples of these attacks are: input, memory, and CPU congestion. These attacks use too long strings of characters, or high traffic load in order to congest the hardware and thus make the device unusable. These attacks can be prevented by using endpoint security tools like [12].

System attacks also include attacks on the *system hardware* like: A/D converter, memory, or passwords. Modification of the A/D converter can alter the measurement accuracy and is very hard to detect. Attack on memory can target various types of memory like: RAM; or memory for measured data, events, OS, or configuration. Password attacks like [13] are used to gain access rights into the device.

D. Attacks on System for Demand Regulation

The demand regulation is a security part of the system responsible for mitigating the network downtimes and therefore increasing the network effectivity. The biggest threats are: high load of the grid network (causing instability and possibly a blackout) and a shutdown of all the devices [10].

E. Attacks on IP

There is a large amount of well-known attacks on the IP. Their list can be found for example in [14]. Most of these attacks are the same or similar for both versions of IP-4 and 6.

The biggest difference between the versions is a new field for additional headers in IPv6, which can be misused for various attacks. Nowadays, the use of IPsec in IPv6 is not required (it is only recommended), making its security very similar to the IPv4.

IV. SOLUTION MODELS OF THE SG RISKS

This section proposes security solutions for the SG risks described in the previous section. These protection recommendation should minimize the risks and can be realized in the current SG networks.

A. Securing Smart Metering Devices

Smart metering devices protection is composed from two parts: mobile communication security and device security.

The communication can be protected by using USSD and Call Barring services implemented in a smart metering devices' SIM. These services can restrict incoming and outgoing calls only to the necessary communication, effectively mitigating SIM's misuse. Additionally, a registration list with SIMs and their corresponding metering device should be used for easy detection of unallowed SIM transfer.

The security of devices can be improved using the following techniques. Checking the data consistency in the control center can eliminate data loss, which can be caused by an attack. An effective monitoring technique via a watchdog device was described in [15]. Authenticated access to the internal database of Smart Grid should be used to protect sensitive information about consumers. Setting modification, on a metering device, via optical interface should be disabled or protected with a physical obstacle (removable only in the case of local reading check by the certified employee of the electricity company). Lastly, communication with a third party should be disabled and a minimal required reading period should be set.

B. Securing IP

IP has to be secured regardless of version used (4 or 6). The following mechanisms are recommended.

IPsec secures communication with authentication and encryption. Authentication verifies if data was send by the legitimate sender, while encryption ensures that only the legitimate receiver can read the message content.

Partial protection against scanning attacks can be achieved with random assignments of IP addresses. On the other hand, it requires additional configuration (ideally using DHCPv6) and it complicates the network addressing. Its usage is therefore recommended only in the critical parts of the SG network, or somewhere, where the risk of the attack is high.

DoS protection can be improved by disabling unneeded services (ICMP, UDP, etc.) and by specification of allowed IP addresses. Typically, broadcast and selected multicast addresses can be safely disabled. If some used systems do not comply with the RFC 5095 standard [16], packets with type 0 routing header should be disabled as well.

MitM is another type of complex protection. One solution is the Secure Neighbour Discovery (SEND). Unfortunately, due to encryption operations, SEND has high computational requirements, making it less suitable for the SG environments [17]. MitM attacks using fake ICMPv6 Neighbour Advertisements can be mitigated by monitoring neighbours' cache memory and notifying about change. Lastly, the fake DHCPv6 server protection should be deployed [18].

Additional security can be achieved if transmitted data is encrypted at the application layer. This layer is offering larger variability in encryption protocols, but it is important to consider performance of end devices (which are responsible for encryption and decryption).

C. Device Authentication

Device authentication is important in order to ensure, that proper devices are present and used within the network. Without the proper authentication, measuring devices could be replaced with fake ones. This would effectively give the attacker a free hand in data being sent into the SG network. Two basic models of authentication can be used, either by hardware address or public key.

Authentication using hardware address integrated into IPv6. This protection is based on the unique identificator (ID) inserted into the IPv6 header. This ID can be generated automatically based on a secret key, MAC address, or unique number in a specialized chip. Unfortunately, this model is using only one-way authentication (client devices towards servers) and cannot be used if some devices do not support IPv6 (which is common in the SG networks).

Authentication using public key. Public key infrastructure (PKI) is a complex solution using asymmetric cryptography. One of the functions of PKI is an electronic signature, which can ensure: identification, authentication, integrity, and non-repudiation. PKI uses certification authorities, which allow to separate management of different parts of the system. If the certification authority for a selected part of the network is hacked, all the other parts of the network are still secured.

V. Conclusion

The usage of Smart Grid networks is expected to rise in the future, especially with the rising demand for electricity. Only intelligent networks like the SG can effectively cope with the variability of these demands, and at the same time ensure reliability and resiliency of the infrastructure. In order to comply with these requirements, perfect security has to be implemented and used.

This paper used a systematic approach to describe the possibilities of the SG attacks on various aspects of these networks. This include attacks on: communication networks, SCADA systems, AMIs, systems for demand regulation, and general IP attacks. The last section described recommended solution models for mitigating the SG risks in the area of smart metering devices, IP networks, and device authentication. It is important to emphasize, that although these recommendations can greatly reduce the risk of an attack, no mechanism can ensure absolute protection. This is especially true for the DoS or MitM type of attacks. It is therefore highly desirable to continue in the SG security research in order to develop and implement more robust security mechanisms. One of the promising ways to achieve this goal can be the area of Software Defined Networks.

Acknowledgment

This work and contribution is supported by the project of the student grant competition of the University of Pardubice, Faculty of Electrical Engineering and Informatics.

References

[1] CEZ: Smart grids (2016), [online] Available: https://goo.gl/xVrKjC, accessed Sep. 29, 2016.

[2] M. Holloway, “Stuxnet worm attack on iranian nuclear facilities,” 2015, [online] Available: https://goo.gl/3ZChrz, accessed Sep. 29, 2016.

[3] S. Khandelwal, “Israeli power grid authority suffers massive cyber attack,” 2016, [online] Available: https://goo.gl/XGyAoC, accessed Sep. 29, 2016.

[4] B. Krebs, “Cyber incident blamed for nuclear power plant shutdown,” 2008, [online] Available: https://goo.gl/vuhKcb, accessed Sep. 29, 2016.

[5] J. Horalek, V. Sobeslav, O. Krejcar, and L. Balik, “Communications and Security Aspects of Smart Grid Networks Design”, in *Cham* 2014, pp. 35-46. Springer International Publishing.

[6] E. Hossain, Z. Han, and H. Poor, “Smart Grid Communications and Networking,” in *Cambridge University Press,* 2012 [online] Available:
https://goo.gl/0A6q3P, accessed Sep. 29, 2016.

[7] T. Flick, and J. Morehouse, “Front matter. In: Securing the Smart Grid,” in *Syngress,* Boston, 2011 [online] Available: https://goo.gl/pvjrN9, accessed Sep. 29, 2016.

[8] C. Bennett, and D. High, “Networking ami smart meters,” in: *Energy 2030 Conference*, 2008. pp. 1-8.

[9] ISO 31000, “Risk management (2009),” [online] Available: https://goo.gl/Xl2Qi1, accessed Sep. 29, 2016.

[10] I. Ghansah, “Smart grid cyber security potential threats, vulnerabilities and risks,” 2012 [online] Available: https://goo.gl/ne3RPn, accessed Sep. 29, 2016.

[11] M. Nathan, “Vodafone femtocells hacked, root password revealed,” 2011 [online] Available: https://goo.gl/njgtPE, accessed Sep. 29, 2016.

[12] L. Balik, J. Horalek, O. Hornig, V. Sobeslav, R. Dolezal, and K. Kuca, “Endpoint Firewall for Local Security Hardening in Academic Research Environment,” in: *Computational Collective Intelligence:*

7th International Conference, ICCCI 2015, pp. 246-255. DOI: 10.1007/978-3-319-24306-1_24

[13] J. Horalek, F. Holik, O. Horak, L. Petr, and V. Sobeslav, “Analysis of the use of Rainbow Tables to break hash,” in: *Journal of Intelligent & Fuzzy Systems*, vol. 32, no. 2, pp. 1523-1534, 2017. DOI: 10.3233/JIFS-169147

[14] F. Aloula, A. Al-Alia, R. Al-Dalkya, M. Al-Mardinia, and W. El-Hajjb, “Smart grid security: Threats, vulnerabilities and solutions,” in: *International Journal of Smart Grid and Clean Energy* [online] Available: https://goo.gl/DEAVWA, accessed Sep. 29, 2016.

[15] H. Pan, E. Hou, and N. Ansari, "M-NOTE: A multi-part ballot based e-voting system with clash attack protection", in *2015 IEEE International Conference on Communications (ICC)*, London, 2015, pp. 7433–7437. DOI: 10.1109/ICC.2015.7249514

[16] IETF, “Deprecation of type 0 routing headers in ipv6,” 2007 [online] Available: https://tools.ietf.org/html/rfc5095, accessed Sep. 29, 2016.

[17] IETF, “Secure neighbor discovery (send),” 2005, [online] Available: https://tools.ietf.org/html/rfc3971, accessed Sep. 29, 2016.

[18] R. Wanner, “A complete guide on ipv6 attack and defense,” 2011, [online] Available: https://goo.gl/f6RbTP, accessed Sep. 29, 2016.