e-mentor
DWUMIESIĘCZNIK SZKOŁY GŁÓWNEJ HANDLOWEJ W WARSZAWIE
WSPÓŁWYDAWCA: FUNDACJA PROMOCJI I AKREDYTACJ KIERUNKÓW EKONOMICZNYCH


2017, nr 1 (68)

Jacob Mendel, Smart Grid Cyber Security Challenges: Overview and Classification, „e-mentor” 2017, nr 1(68), s. 55–66, http://dx.doi.org/10.15219/em68.1282.

# Smart Grid Cyber Security Challenges: Overview and Classification

*Jacob Mendel*

*The Smart Grid is gradually attracting the attention of government, industry and academia. It is a next generation electricity network that depends on two-way communication between its elements, being more reliable, more efficient and self-healing, with automatic meter reading and dynamic pricing*[1]*. Smart Grid technology presents new cyber security threats that should be addressed. Deploying a Smart Grid without suitable cyber security might result in serious consequences, such as grid instability, utility fraud, and the loss of user information and energy consumption data. Due to the various architectures that assure communication within the Smart Grid, it is a challenge to design an advanced and strong cyber security concept that can be smoothly deployed to protect the devices in the Smart Grid's infrastructure. This article focuses on Smart Grid cyber security threats to Home Area Networks (HANs) and Neighbourhood Area Networks (NANs). It aims at providing knowledge management and deep analysis of the threats to HANs and NANs, including one of the biggest cyber security threats, advanced malware. Smart Grid Malware mitigation is essential to ensure the proper functioning and efficient operation of the utility companies and the private home economy. Advanced malware has a variety of anti-detection features like dynamic encryption, code obfuscation and stealth operation. The offensive part of advanced malware has a mechanism to disguise who, when and where will be attacked.*

The Smart Grid is one of the most critical infrastructure services of today's nation state, so comprehensive cyber security and privacy mechanisms are needed to guarantee its continuous and reliable operation. The new smart metering is the gateway between the Smart Grid and our homes or businesses, enabling dynamic pricing (NIST 2014) and information exchange with smart home devices (IoT), which are all connected.

Despite its critical importance, research on smart home and Smart Grid security issues is still in its early stage. As a result, we are motivated to investigate Smart Grid cyber security issues further [2]. Cyber-security, both for critical infrastructure in general and for the Smart Grid, which is a fundamental element of it, is a very troubling issue because the number of attacks on critical infrastructure is continuously increasing. According to an NCCIS report[3], ICS-CERT responded to 295 cyber incidents (Figure 1), the majority of them (230) first detected in the business networks of critical infrastructure organizations. Some 59% of the reported incidents occurred in the energy sector, which exceeded all the incidents reported in other sectors combined.

A key element of the Smart Grid is the availability of Advanced Metering Infrastructure (AMI), with a constant and stable connection to the utility company. This paper attempts to provide an overview of the main cyber security threats to the Smart Grid with a focus on the smart meter. Its goal is to present a summary of the state-of-the-art smart meter cyber security threats and provide a better understanding of the direction of future research which is required in this field. Most of the topics mentioned in the paper can be extended to other areas of cyber security research, educational applications/knowledge management and different industries.

Threats can be defined as the range of possible actions that can be taken against a system[4]. They can

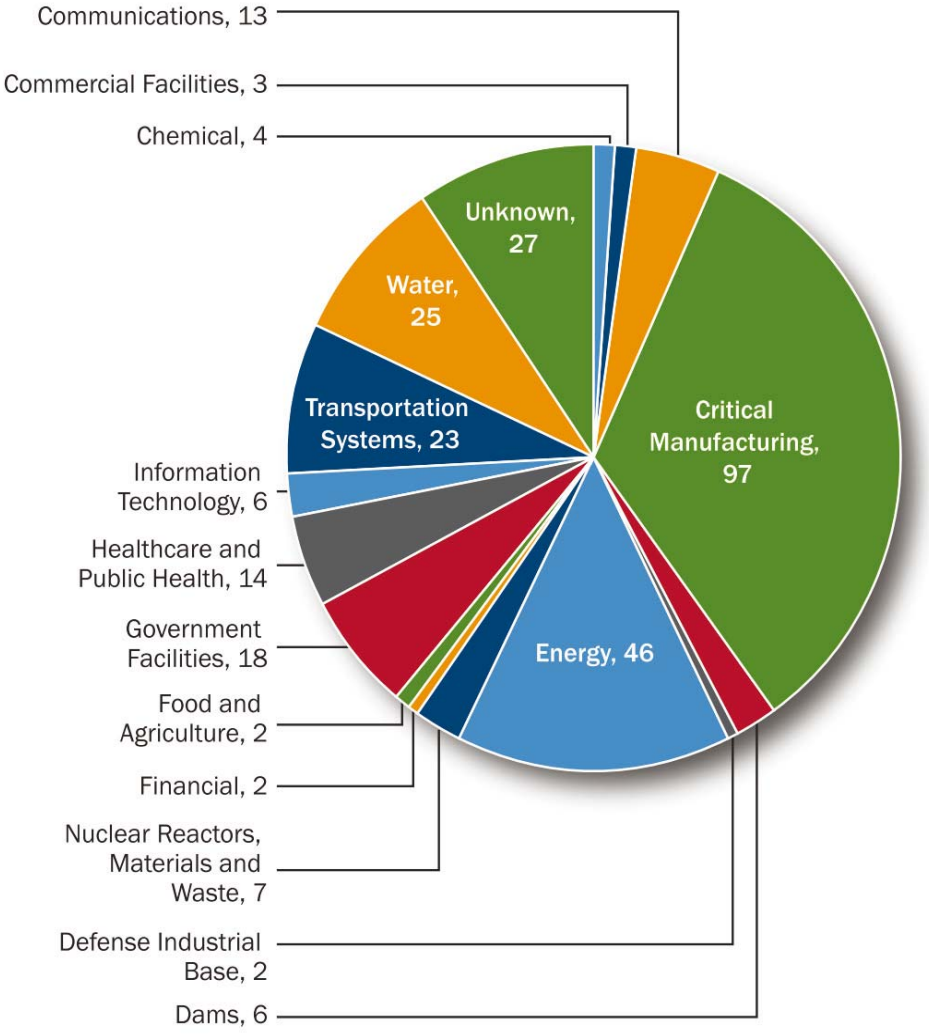
[1] F. Skopik, Z. Maa, T. Bleiera, H. Grüneisb, *A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures*, „International Journal of Smart Grid and Clean Energy" 2012, pp. 22–28, http://www.ijsgce.com/index.php?m=content&c=index&a=show&catid=27&id=16, [12.12.2016].

[2] N. Komninos, E. Philippou, A. Pitsillides, *Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures*, „IEEE Communications Surveys & Tutorials" 2014, Vol. 16, No. 4, pp. 1933–1954, http://dx.doi.org/10.1109/COMST.2014.2320093.

[3] *NCCIC/ICS-CERT Year in Review*, National Cybersecurity and Communications Integration Center/Industrial Control Systems Cyber Emergency Response Team, U.S. Departament of Homeland Security, 2015.

[4] *Protecting Industrial Control Systems. Annex I*, ENISA, 2011.

**Figure 1. ICS-CERT incidents reported in 2015**




Source: *NCCIC/ICS-CERT Year in Review*, National Cyber-security and Communications Integration Center/Industrial Control Systems Cyber Emergency Response Team, U.S. Department of Homeland Security, 2015.

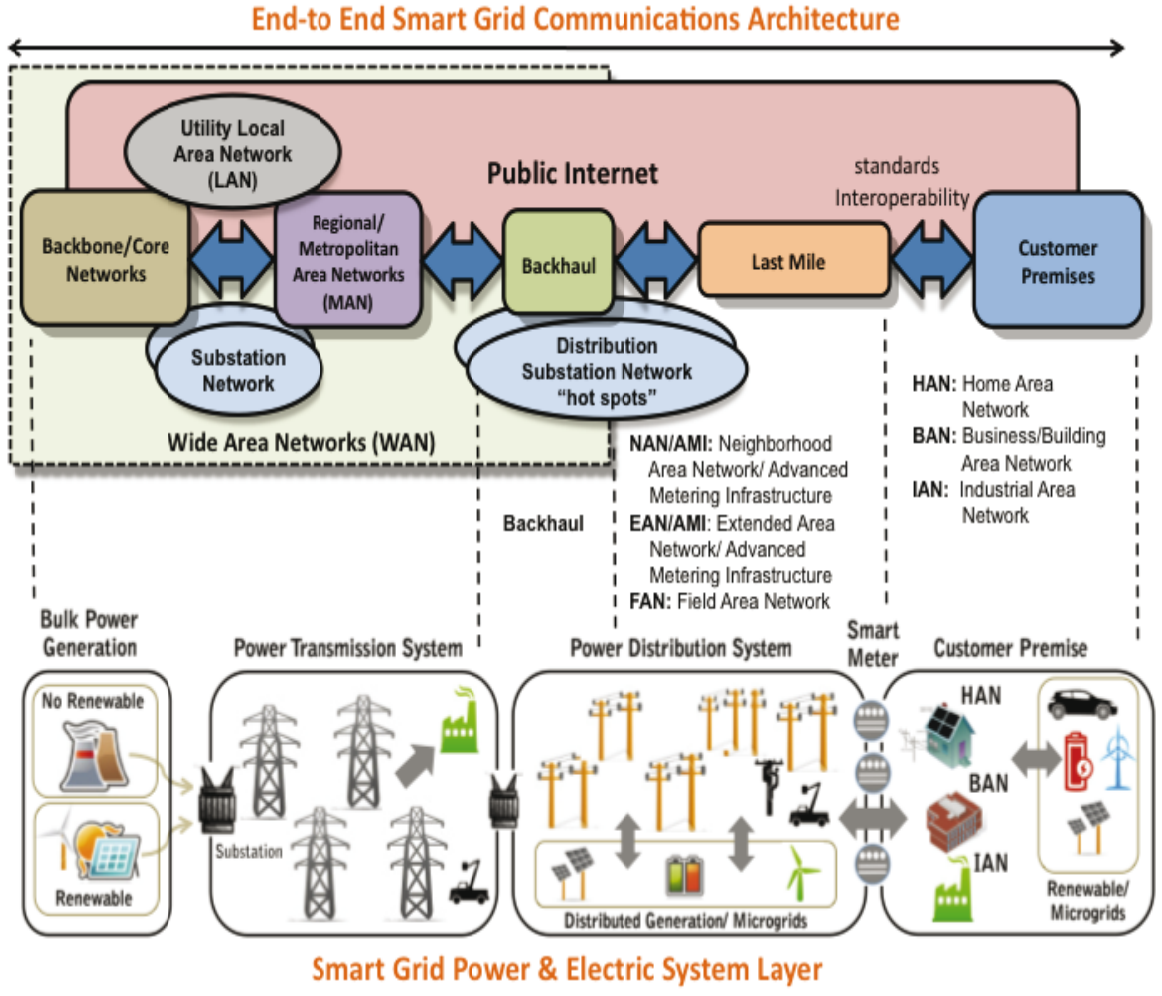
be classified according to different criteria, for example: accidental or deliberate actions (safety failures, equipment failures, carelessness, natural disasters), insider or outsider (criminal groups, terrorists, nation-states/foreign intelligence services), or by the techniques of attack (physical destruction, theft, malware, communication threats, escalation of privileges, data base injection, denial of service, replay, spoofing, social engineering, phishing, spam). In this paper, the attention of the author will be focused on the malware that could affect the Smart Grid. According to the ENISA 2016 report, malware remained the number one cyber-threat, increasing to one million new samples per day and one can assume that it will remain one of the top three threats in 2017.

## Smart Grid Communication components

The Smart Grid communication infrastructure is divided into four sub-networks[5], which are: Wide Area Networks (WANs), Neighbourhood Area Networks (NANs), Small Business Networks (SBNs) and Home Area Networks (HANs). A similar approach has been presented by the NIST[6], whereby the Smart Grid is a system of systems (Figure 2) and a combination of multiple different technologies and layers,

[5] H. Wen, Y. Wang, X. Zhu, J. Li, L. Zhou, *Physical layer assist authentication technique for smart meter system*, „IET Communications" 2013, Vol. 7, No. 3, pp. 189–197, http://dx.doi.org/10.1049/iet-com.2012.0300.
[6] *NIST, 2009. NIST The Role of the Internet Protocol (IP) in AMI Networks for Smart Grid.*, p. 16.

**Figure 2. Smart Grid Communications Architecture**




Source: *NIST, 2009. NIST The Role of the Internet Protocol (IP) in AMI Networks for Smart Grid.*, p. 16.

which require interfaces between these segments to be properly defined and harmonized. A Wide Area Network (WAN) is used to connect multiply Home Area Networks in order to collect and manage data transmission for measurement and control purposes. A Neighbourhood Area Network (NAN) connects multiple SBNs and HANs together. SBNs, HANs and NANs belong to the Advanced Metering Infrastructure (AMI). A Small Business Network (SBN) and a Home Area Network (HAN) connect all the home/small business appliances and most commonly use short-range area wireless transmission to support real-time meter data transfer, dynamic pricing and deterministic direct load control. It was decided that the same approach to SBN and HAN be taken because they are similar, just as in the research undertaken by D. He et al.[7]. One of the main Smart Grid cyber security challenges is securing the smart meter.

## Neighbourhood Area Networks (NANs)

Neighbourhood Area Networks (NANs) may be defined as networks that cover small geographical areas and are responsible for the interconnection of smart meters from a variety of premises with multiple access points that aggregate the data collected by smart meters, forwarding it to the upper layer[8]. According to D. He et al.[9], an essential part of the Smart Grid is its communication network. This is a three-tier

[7] D. He et al., *An enhanced public key infrastructure to secure smart grid wireless communication networks*, „*IEEE Network" 2014*, Vol. 28, No. 1, pp. 10–16, http://dx.doi.org/10.1109/MNET.2014.6724101.
[8] N. Komninos, E. Philippou, A. Pitsillides, op.cit.
[9] D. He et al., op.cit.

(i.e. NAN, BAN, HAN) network, which connects the different components of the Smart Grid together, and allows bi-directional communication. The first tier connects the communication system located at the power plant and the control centres of the Neighbourhood Area Network (NAN). The second tier is the NAN that comprises a number of Building Area Networks and provides them with interfaces to the utility's Wide-Area Network (WAN). The third tier is the Home Area Network (HAN) that connects all the home devices to one gateway.

### Home Area Networks (HANs)

According to Jokar[10], Home Area Networks (HANs) are the subsystems within an Advanced Metering Infrastructure (AMI), which are responsible for the data transfer among smart meters and household electrical devices and appliances. In many countries, wireless is the dominant technology for HANs. The shared media used by wireless networks make them inherently more vulnerable to cyber security threats when compared with wired networks. In addition, an HAN is located in public areas, which makes it an easily accessible target for malicious attackers. At the same time, due to the resource and computational limitations of HAN devices, implementation of strong cyber security protection concepts is a challenging task.

A. Ajayi, B. Alese, S. Fadugba and K. Owoeye[11] suggest another view of Home Area Networks (HANs) that includes communicating Smart Grid components such as: Smart Thermostats, Smart Water Heaters, Smart Appliances and Plug-in Hybrid Electric Vehicle (PHEV)/storage. All the HAN devices are connected to a smart meter through a network such as ZigBee or mesh wireless. The smart meter connects the HAN to a collector node, also through a WiFi network such as ZigBee (IEEE 802.15.4), Z-Wave, Bluetooth Low Energy (BLE) or any other proprietary mesh wireless, and may also communicate with the other nearby HAN networks. Collector nodes communicate with the utility through different means of communication, including the Internet.

### Smart meters

A smart meter, according to X. Fan and G. Gong[12], is composed of a microcontroller, a metering board and a communication board. Under the control of the microcontroller, the metering board measures real-time power consumption, and the meter data is transmitted to both the substation network as well as the home area network through the communication board. The connection between the smart meter and the home appliances may be through Wi-Fi, ZigBee, Ethernet, HomePlug, Wireless M-Bus, etc. The smart meter may also contain a disconnect function that (if enabled) allows utility companies or customers to remotely connect or disconnect home appliances and services.

According to the following classification[13], the features of smart metering functionality are:

- Measuring power usage in real-time, recording it and sending these registers to the utilities company or other third party providing energy services;
- Monitoring and informing the utility company, the customer and third parties about power quality;
- Tracking customer usage parameters, such as total energy consumption, and keeping a historical record;
- Remotely connecting and disconnecting customers from the power grid;
- Sending out alarms to the utility company where there are technical issues such as component failure or loss of power notifications;
- Reacting to real-time pricing signals received from the utility company or energy retailer;
- Energy prepayment;
- Remotely receiving and installing firmware upgrades so as to incorporate new functionality;
- Anti-tampering and fraud detection;
- Remotely customizable load limit feature.

Based on the above-mentioned description, it is clear that the smart meter is a critical cyber security component, which requires special protection, especially as it is also the gateway to the entire Smart Grid system, and in some cases it is the Smart Home gateway. The Advanced Metering Infrastructure (AMI) network is used to connect customers' homes, the utility centre and the electricity market.

Faisal[14] defines Advanced Metering Infrastructure (AMI) as an imperative component of the Smart Grid, as it is responsible for collecting, measuring and analysing energy usage data, and transmitting this data to the data concentrator and then to a central system in the utility headquarters. Therefore, the cyber security of AMI is one of the most challenging issues in Smart

[10] P. Jokar, *Model-based Intrusion Detection for Home Area Networks in Smart Grids*, http://blogs.ubc.ca/computersecurity/files/2012/04/PJokar_HAN_IDS_-_Paria.pdf, [30.11.2014].
[11] A. Ajayi, B. Alese, S. Fadugba, K. Owoeye, *Sensing the Nation: Smart Grid's Risks and Vulnerabilities*, „International Journal of Communications, Network and System Sciences 2014, Vol. 7, No. 5, pp. 151–163, http://dx.doi.org/10.4236/ijcns.2014.75017.
[12] X. Fan, G. Gong, *Security Challenges in Smart-Grid Metering and Control Systems*, „Technology Innovation Management Review" 2013, Vol. 3, No. 7, pp. 42–49.
[13] Ibid., E. Egozcue et al., 2012. *Annex I. Smart Grid Security,* enisa, (April), p. 59.
[14] M.A. Faisal et al., *Securing Advanced Metering Infrastructure Using Intrusion Detection System with Data Stream Mining*, [in:] „Intelligence and Security Informatics. Proceedings Pacific Asia Workshop", PAISI 2012, pp. 96–111, http://dx.doi.org/10.1007/978-3-642-30428-6_8.

Grid implementation. It has been clearly defined that malware intrusion detection system (IDS) architecture for AMI will act in a complementary way to other cyber security measures in the Smart Grid.

The NIST[15] suggests the following approach to AMI. Advanced Metering Infrastructure (AMI) provides near real-time monitoring of power usage, and is a current focus of utilities. These advanced metering networks are of many different designs and could also be used for residential demand response, including dynamic pricing. AMI consists of communications, and the related system and data management, that together create the connection between the advanced meters and the utility system, enabling collection and distribution of information to customers and other parties (like: competitive retail).

## Cyber attacks on smart meters

The smart meter vulnerabilities suggested by F. Skopik, Z. Maa, T. Bleiera and H. Grüneisb[16] are exploited by attacks on the smart meter itself and/or its interfaces in several ways, either by:

1. Manipulating the hardware: Current smart meters are designed to continue valid operation even if the communication with the utility, the data centre or the collector node has been lost. This is mandatory for ensuring smooth operation in cases of communication disruptions. Thus, shielding the antenna of a wireless module (e.g. WiFi 802.11 or ZigBee 802.15.4) or using an electrical filter to suppress the high frequencies of a modulated signal on the power line is a first step towards preventing remote meter readings (i.e. DoS). Furthermore, once a smart meter's housing has been successfully opened, opportunities to gain access to the firmware might arise, for instance, through an unsecured ISP port or lock bit attack methods. Finally, exchanging smart meter devices between different locations, replacing smart meters with cloned devices, or at least their communication modules, can cause inaccurate accounting and billing.
2. Manipulating the firmware: These attacks aim at modifying the smart meter operating system program flow, e.g. by interrupting the internal and external power supply, or by exploiting a local service port. Smart meter producers invest much effort into preventing such attacks, e.g. by checking the consistency and anomaly of the smart meter readings or by sending a „heart beat" signal at periodic time intervals. However, reprogramming of the actual firmware located in the smart meter's flash memory by skilled attackers with insider knowledge is also possible.
3. Exploiting limitations in design and implementation: Although many security concepts exist and a system may be securely designed (at an appropriate level), usually, some conditions are not fully considered and failures in actual implementation, for instance, the transmission of encryption keys over unencrypted channels, can happen. One may assume that even if smart meter manufacturers adopt and integrate secure code development[17], a variety of authentication methods, strong encryption for communication, as well as secure key management, secure boot loaders and code running integrity checks, all of this will still not prevent advanced malware attacks.

According to Aloul & Al-Ali[18], smart meter vulnerabilities are among the most serious in Smart Grids. The vulnerabilities that apply to smart meters are:

1. Customer security: Smart meters autonomously collect massive amounts of end user data and transmit it to the collector, utility company, consumer and service providers. This data includes private consumer information that might be used to infer a consumer's activities, devices being used, and times when the home is vacant.
2. Physical security: Unlike the traditional power system, the Smart Grid network includes many distributed components, with some of them being out of the utility's premises. This fact increases the number of insecure physical locations and makes them vulnerable to physical access and attack.
3. Implicit trust between traditional power devices: Device-to-device communication in control systems is vulnerable to data spoofing, where the state of one device affects the actions of another device. For example, an attacker can disturb the service availability of a customer by sending false control signals to the sensor nodes or false usage data to the smart meters[19].

[15] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, *Guide to Industrial Control Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)*, National Institute of Standards and Technology, U.S. Departament of Commerce, 2015, http://dx.doi.org/10.6028/NIST.SP.800-82r2.

[16] F. Skopik, Z. Maa, T. Bleiera, H. Grüneisb, op.cit.

[17] F. Skopik, P. Smith, *Secure Development Life Cycle*, [in:] *Smart Grid Security. Innovative Solutions for a Modernized Grid*, Elsevier, Waltham 2015.

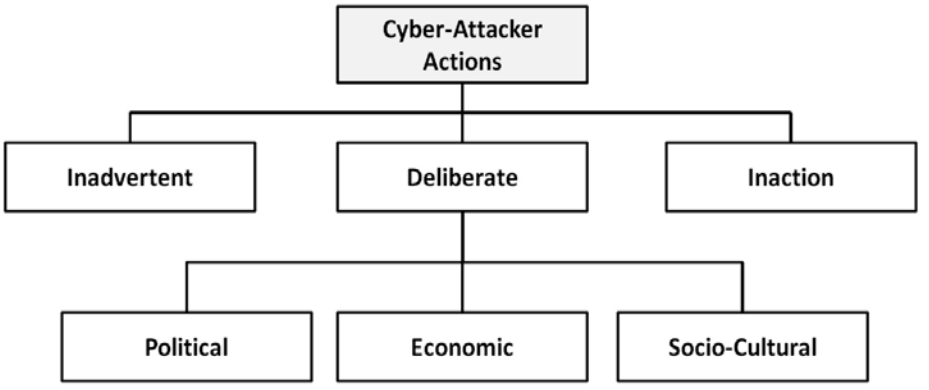
[18] F. Aloul, A. Al-Ali, *Smart grid security: Threats, vulnerabilities and solutions*, „International Journal of Smart Grid and Clean Energy Smart" 2012, Vol. 1, No. 1 (September), p. 6, http://dx.doi.org/10.12720/sgce.1.1.1-6.

[19] P. Jokar, op.cit.

4. An attacker can develop advanced malware or simply modify existing malware and spread it to infect the Smart Grid. The malware can be used to modify system settings, or infect other files on the system[20].

The primary concern[21] of companies and organizations are cyber attacks that are deliberate actions, which have been categorised based on the motivations behind them (Figure 3). According to the Verizon[22] data breach report, the financial motivation (for example theft of intellectual property or users' private information or credit card information) is one of the strongest motivations for attacks. Political and espionage motivations are categorized immediately after and involve, for example: destroying important web sites, disrupting – i.e. DDOS attacks, taking control of strategic or symbolic targets, blackouts or making political statements.

**Figure 3. Types of cyber-attacker actions**




Source: Han & Dongre 2014.

## Standardization

There are hundreds of different standards in the Smart Grid field[23]. It is extremely important to comply with the relevant national standard, especially to ensure interoperability. In this paper one of the most important Smart Grid security standards – IEC 62351 will be covered. This standard defines data and communication security handling for the International Electrotechnical Commission (IEC) Technical Committee 57. TC 57 is responsible for developing standards for Smart Grid and power systems. IEC 62351 is a standard developed by WG15 of IEC TC57, that includes, the IEC 60870 series, IEC 61850 series, IEC 61970 series & IEC 61968 series. These long lists of standards do not solve the problem of the security of the Smart Grid but provide a very good starting point for a variety of players in this field to address cyber security threats and create minimum-security requirements in the critical Smart Grid.

### IEC 62351

According to T. Baars et al.[24], IEC 62351 is a standard for data and communication security. It is being developed by IEC Technical Committee 57 for the purpose of providing information security for power system control operations. Its primary objective in a broad sense is to take on the development of standards and/or technical reports defined by IEC Technical Committee 57 on end-to-end security issues. The reason IEC 62351 is being developed is the increasing need for safety, security and reliability and the awareness that ensuring end-to-end security requires more than simple technological measures. Additionally, the current standards are not prepared for containing security measures. The 62351 series serves as an umbrella for IEC 60870-5, IEC 60870-6 and IEC 61850 standards in the areas of authentication and communication security.

[20] M. Egele, T. Scholte, E. Kirda, Ch. Kruegel, *A survey on automated dynamic malware-analysis techniques and tools*, „ACM Computing Surveys (CSUR)" 2012, Vol. 44, No. 2, pp. 1–42, http://dx.doi.org/10.1145/2089125.2089126.
[21] C. Han, R. Dongre, *Q&A. What Motivates Cyber-Attackers?*, „Technology Innovation Management Review" 2014, Vol. 4, No. 10, pp. 40–43.
[22] *Data Breach Investigations Report*, Verizon 2016, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf, [12.12.2016].
[23] T. Sato et al., *Smart Grid Standards: Specifications, Requirements, and Technologies*, Wiley, 2015, http://dx.doi.org/10.1002/9781118653722.
[24] T. Baars et al., *Cyber Security in Smart Grid Substations*, Technical Report UU-CS-2012-017, Department of Information and Computing Sciences, Utrecht University, Utrecht 2012.

### Advanced Metering Infrastructure Security (AMI-SEC)

According to NIST SP 1108R2[25], the Advanced Metering Infrastructure Security (AMI-SEC) Task Force was established under the Utility Communications Architecture International Users Group (UCAIug) to develop consistent security guidelines for Advanced Metering Infrastructure (AMI). This document provides security guidance to organizations developing or implementing AMI solutions. This includes the meter data management system (MDMS) up to and including the HAN interface of the smart meter. Unfortunately, this guideline has not been updated since December 2009.

Mere compliance with cyber security standards will not assure security. It is assumed that large utilities will use applicable industry standards and best practices, including emerging security standards like NIST's Smart Grid Interoperability Standards Framework and AMI-SEC System Security Requirements, for end-to-end security of the Smart Grid. Most will implement intrusion detection and prevention services (IDS/IPS) as well as security information event management (SIEM). They will probably use a system-of-systems approach to cyber security by deploying the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC), National Security Agency InfoSec Assessment Methodology (NSA IAM), the Information Systems Audit and Control Association (ISACA), and the International Information Systems Security Certification Consortium (ISC2). This has been stated by Gellings[26] and does not bring the expected cyber security solution to the Smart Grid.

### Common Criteria

The Gateway is the central communication unit in the smart metering system (Common Criteria, Smart Meter Gateway PP, BSI-CC-PP-0073, V1.3, 31-March 2014). It should be the only unit directly connected to the WAN, to be the first line of defence an attacker located in the WAN would have to conquer. The gateway is the central component that collects, processes, and stores meter data. It is therefore the primary point for user interaction in the context of the smart metering system. This protection profile defines the security objectives and the gateway requirements, which are the main communication components of such a smart meter system. The target of evaluation (TOE) that is described in the protection profile is the smart meter gateway hardware and software/firmware used for smart meter data collection, data storage and provisioning. The secure element is excluded from the TOE. According to the protection profile, the smart meter gateway makes the connection between the Wide Area Network (WAN) and the Home Area Network (HAN) to other smart meters. The security functions of the TOE according to the protection profile are: protection of confidentiality and authenticity; integrity of data and information flow control; protection of the privacy of the smart meter consumer; ensuring a reliable billing process. It is interesting to note that the protection profile does not address smart meter availability although it is a clear cyber security threat, which should be included.

## Smart Grid cyber security threats

Cyber security for critical infrastructure in general and for Smart Grid in particular is an issue of much concern because of emerging cyber threats. Smart Grid cyber security is of fundamental importance to modern society. In fact, if one (or more) of the Smart Grid cyber security threats are successfully implemented it may harm the entire Smart Grid, causing economic damage and bad societal influence. According to N. Komninos, E. Philippou and A. Pitsillides[27], the security of the Smart Grid has become a primary concern for modern society.

Smart Grid cyber security threats can come from a myriad of sources, such as: cyber crime[28], hacking[29] and cyber war[30]. To mitigate cyber security threats, utility companies will need to share and coordinate the exchange of cyber security information, like intelligence and vulnerabilities, with governmental agencies (for example: ICS-CERT – the Computer Emergency Response Team) and probably with other public and private sector cyber research institutes. Through such cooperation and with a holistic approach that includes on-going cyber security self-improvement, the Smart Grid's critical services will be protected.

X. Li[31] suggests a way of preventing potential cyber attacks on Smart Grid communication by identifying four types of attack: a device attack (aims to compromise a grid device), a data attack (attempts to maliciously insert, alter or delete data or control commands in the network traffic to misguide the

[25] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, op.cit.
[26] C. Gellings, *Estimating the costs and benefits of the smart grid*, EPRI, 2011, p. 162.
[27] N. Komninos, E. Philippou, A. Pitsillides, op.cit.
[28] R.J. Baijusha, R. Ganeshan, *Cyber-physical system security using decoy system*, http://ijartet.com/, [6.03.2017].
[29] M. Wagner, M. Kuba, A. Oeder, *Smart grid cyber security: A German perspective*, 2012 International Conference on Smart Grid Technology, Economics and Policies (SG-TEP), Nuremberg 2012, http://dx.doi.org/10.1109/SG-TEP.2012.6642389.
[30] T. Baars et al., op.cit.
[31] X. Li et al., *Securing smart grid: cyber attacks, countermeasures, and challenges*, ,,IEEE Communications Magazine" 2012 (August), Vol. 50, No. 8, pp. 38–45, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6257525 [6.03.2017], http://dx.doi.org/10.1109/MCOM.2012.6257525.

Smart Grid, leading it to make wrong decisions/actions), a privacy attack (aims to learn/infer users' private information by analysing electricity usage data), and a network availability attack (i.e. a DoS – Denial of Service). They have different objectives and are often the building blocks of more sophisticated attacks.

In an alternative approach, K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams and A. Hahn[32] propose their own model for threat sources, vulnerabilities and incidents within Smart Grid industrial control systems (ICS). Their model provides fine details of each cyber security threat source, including a description of the characteristics of each type of threat. It was decided that this paper should focus on the malware threat to Smart Grids, especially in the smart meter environment.

A similar opinion seems to be shared by Hahn[33]. Attacks on the Smart Grid will likely differ from the many traditional attacks on cyber environments. First, an attacker must be able to compromise the grid's cyber elements. However, in order for the attack to cause negative system impact, the attacker must also know how to control the cyber elements to manipulate the physical system. In his description of system attacks, Hahn[34] also refers to software vulnerabilities (such as buffer overflows, integer overflows and structured query language – SQL injection). Many devices within the Smart Grid do not use strong methods to authenticate users. Such threats may provide an attacker with the ability to bypass the authentication and take control of the Smart Grid network. To address user authentication for accessing the Smart Grid, Q. Gao[35] recommended strengthening user authentication against these types of attacks by employing three factors of authentication: something you know (knowledge-based), something you have (possession-based), and something you are (biometrics-based). Multi-factor authentication refers to the combining of two or three of these factors. An additional factor of user authentication for a Smart Grid can be: keystroke, voice, signature, iris, face, fingerprint or behavioural authentication. The Smart Grid cyber security threats are summarised in table 1.

**Table 1. Smart Grid Cyber Security Threats**

| Cyber Security Threats in the Smart Grid | |
|---|---|
| **Threat** | **Description** |
| Availability | • Denial of Service (DoS) (on an individual device, a group of devices or an entire sub network) e.g. (Stelte B., Rodosek G.D., *Thwarting attacks on ZigBee – Removal of the KillerBee stinger*, [in:] *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*, Zurich 2013, pp. 219–226)<br>• Communication hijacking/MITM attacks e.g. (Beasley C., Venayagamoorthy G.K., Brooks R., *Cyber Security Evaluation of Synchrophasors in a Power System*, 2014)<br>• Jamming e.g. (Komninos, N., Philippou, E. & Pitsillides, A., 2014. *Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures*. ,,IEEE Communications Surveys & Tutorials", Vol.16, No.4, pp. 1933–1954)<br>• Device theft e.g. (U.S. National Institute of Standards and Technology, 2014. Guidelines for Smart Grid Cybersecurity NISTIR 7628 Revision 1. *U.S. Department of Commerce NISTIR*, 1(September), p. 668) |
| Integrity | • Vulnerabilities in common protocol e.g. Zhou L., Chen S., *A Survey of Research on Smart Grid Security*, [in:] Lei J., Wang F.L., Li M., Luo Y. (eds), *Network Computing and Information Security. Communications in Computer and Information Science,* Springer, Berlin–Heidelberg 2012)<br>• Protocol manipulation including packet loss e.g. (Stouffer K., Pillitteri V., Lightman S., Abrams M., Hahn A., *Guide to Industrial Control Systems (ICS) Security.* National Institute of Standards and Technology, U.S. Department of Commerce, 2015)<br>• Fraud, Stealthy manipulation of critical data such as meter readings, billing information, control commands.<br>• Tampering (physical attack, Tamper-Event Detection, Device Cloning) e.g. (Iyer S., *Cyber Security for Smart Grid , Cryptography , and Privacy*, „International Journal of Digital Multimedia Broadcasting" 2011) |
| Confidentiality | • Privacy (Identification of Household Activities from Electricity Usage Data) e.g. (Fan X., Gong G., *Security Challenges in Smart-Grid Metering and Control Systems*, „Technology Innovation Management Review" 2013)<br>• Use of power usage data and customer account information |

[32] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, op.cit.
[33] A. Hahn, *Cyber security of the smart grid: Attack exposure analysis, detection algorithms, and testbed evaluation*, 2013.
[34] Ibid.
[35] Q. Gao, *Biometric authentication in Smart Grid*, 2012 International Energy and Sustainability Conference (IESC), Farmingdale 2012, http://dx.doi.org/10.1109/IESC.2012.6217197.

**Table 1 – cont.**

| Cyber Security Threats in the Smart Grid | |
|---|---|
| **Threat** | **Description** |
| Confidentiality | • An emerging trend is for smart meters to aggregate usage data for billing purposes and support load-balancing and other monitoring functions<br>• Backdoors and holes in the network perimeter e.g. (Zaddach J., Bruno L., Francillon A., *Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares*, 2014)<br>• Database attacks e.g. (Beasley C., Venayagamoorthy G.K., Brooks R., *Cyber Security Evaluation of Synchrophasors in a Power System*, 2014)<br>• Protecting the smart meters' data<br>• Spoofing system operators and/or SCADA devices<br>• Leakage of sensitive information (Knapp E.D., Langill J.T., *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid*, *SCADA, and Other Industrial Control Systems,* Elsevier, Waltham 2015) |
| Timeliness | • Real-time needs of control systems and responsiveness aspects of the system e.g. (*NIST Framework and Roadmap for Smart Grid Interoperability Standards. Release 2.0*, National Institute of Standards and Technology, 2014) |
| Human Machine Interface (HMI) | • Fraudulent information about demand or supply which will create non-existing power flows which may result in blackouts and heavy financial losses e.g. (Zaddach J., Bruno L., Francillon A., *Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares*, 2014) |
| Software Vulnerabilities | • Buffer overflows e.g. (Demme J. et al., *On the feasibility of online malware detection with performance counters*, [in:] *Proceedings of the 40th Annual International Symposium on Computer Architecture – ISCA '13*, ACM, New York 2013)<br>• Integer overflows e.g. (Chaffin M.N., *Common Cybersecurity Vulnerabilities in Industrial Control Systems*, U.S. Departament of Homeland Security, 2011)<br>• SQL injection e.g. (Bilge L., Dumitras, T., *Before We Knew It: an Empirical Study of Zero-Day Attacks in the Real World*, 2012)<br>• Code behaviour analysis e.g. (Lukas D., Kroustek J., Zemek, P., *Psyb0t Malware: A Step-by-Step Decompilation Case Study*, 2013)<br>• Software infected with malware which will disrupt the performance of devices or all devices e.g. Hawk C., Kaushiva A., *Cybersecurity and the Smarter Grid*, „The Electricity Journal" 2014) and (Genge B., Rusu D.A., Haller P., *A connection pattern-based approach to detect network traffic anomalies in critical infrastructures,* 2014)<br>• Changes to the software or modifications to the software configuration settings<br>• Changes in programmable logic in PLCs, RTUs, or other controllers (Knapp E.D., Langill J.T., *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid*, *SCADA, and Other Industrial Control Systems,* Elsevier, Waltham 2015) |
| Authentication | • Weak (or none) Password / Authentication e.g. (Komninos N., Philippou E., Pitsillides A., 2014. *Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures*, ,,IEEE Communications Surveys & Tutorials", Vol. 16, No. 4, pp.1933–1954)<br>• Weak (or none) Identification<br>• Weak (or none) Access Control e.g. (Ajayi A., Alese, B., Fadugba S., Owoeye K., *Sensing the Nation: Smart Grid's Risks and Vulnerabilities*, „International Journal of Communications, Network and System Sciences" 2014) |

Source: Komninos N., Philippou E., Pitsillides A., *Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures*, ,,IEEE Communications Surveys & Tutorials" 2014, Vol. 16, No. 4, pp. 1933–1954.

## Malware

According to NIST special publication 800-82[36], early malware threats were primarily viruses, and the software to detect and remove malware has historically been called „antivirus software", even though it can detect many types of malware. Antivirus software is used to counter the threats of malware by evaluating files on a computer's storage devices (some tools also detect malware in real-time at the network perimeter and/or on the user's workstation) against a database of malwares signature files. If one

[36] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, *NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security*, 2015 (May), p. 247, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf., [6.03.2017].

of the files on a computer matches the signature of known malware, the malware is removed through a quarantine process so it cannot infect other files or communicate across the network to infect other files. There are techniques based on anomaly detections to identify unknown malware when a malware signature is not yet available. According to the NIST SP800-82[37], many end-users and vendors of Industrial Control Systems (ICS) are recommending the use of commercial off-the-shelf (COTS) antivirus software with their installation and configuration guidance based on their own laboratory testing. Some Industrial Control Systems (ICS) vendors recommend the use of antivirus software with their products, but offer little to no guidance. Some Smart Grid users and vendors are hesitant about using antivirus software due to worries that its use may cause performance problems or even a failure of Smart Grid devices. NIST and Sandia National Laboratories (SNL) conducted a study and produced a report aimed at helping Industrial Control System (ICS) owners/operators to deploy antivirus software and to minimize and assess the performance impacts of workstation and server-based antivirus products. That study accumulated ICS-based antivirus know-how and assists as a starting point or a secondary resource when installing, configuring, running and maintaining antivirus software on an ICS. In many cases, performance impacts can be reduced through configuration settings, antivirus scanning and maintenance scheduling outside of the antivirus software practices recommended for typical IT systems. Commercial, off-the-shelf (COTS) antivirus software can be used successfully on most Smart Grid components. However, special Smart Grid/ICS specific considerations should be well thought through during selection, installation and configuration, as well as operational and maintenance procedures. Smart Grid component users should consult with vendors regarding the use of antivirus software.

Dai[38]suggests a more comprehensive approach. Malware is a newly coined term for malicious software that is intentionally designed to disrupt availability, compromise confidentiality, alter integrity and cause abusive behaviours. Typically, malware is a general term that covers the range from programming scripts to active executable content, malicious JavaScript and other malicious elements of programming code. Research studies show that the impact of malware infection often not only leads to loss of privacy and confidentiality of data but also allows hackers to abuse the victim's computational resources when conducting larger-scale cybercrime activities. Therefore, malware must be addressed seriously so that financial losses (which could be as high as 0,5 to 1.0% of global gross domestic product) due to malware infection can be avoided.

B. Genge, D.A. Rusu and P. Haller[39] suggested using anomaly detection techniques to identify malware attacks on Smart Grid. Their approach automatically generates detection rules for the IDS (Intrusion Detection System), which relies on predictive behaviour among Smart Grid devices in order to identify abnormal communications. Intrusion Detection Systems (IDS) based on anomaly detection have limitations. They should be applied to narrow Smart Grid traffic in order to be very effective (i.e. low false positive) in detecting abnormal activities. Their anomaly detection relies on the deviation of current communication patterns from normal communication. A significant improvement to Genge, Rusu and Haller's approach can be achieved by adding network traffic visualization and device identification, which can very quickly highlight an abnormal network connection that should not normally exist. To protect the Smart Grid against malware, E.D. Knapp and J.T. Langill[40] suggested that both host-based and network-based security controls should be used. Because of malware changing and disguise, multiple layers of defence are recommended, and all anti-malware efforts should be fully managed and controlled including continuous patching and updates.

Before developing countermeasures against malware, it is important to understand how malware behaves, spreads and attacks; and what type of anti-detection techniques it might use. Applying malware detection software is a time consuming operation, which slows down Smart Grid devices throughout and is not scalable to the growing quantities of advanced malware. One approach that is trying to address this problem uses „fast-clock-running", hoping to trigger the malware's malicious action in advance. However, such an action can be identified by the advanced malware, which will then bypass this check. The most common malware detection methods are:

- Pattern based – like different hash functions (MD5, SHA1, SHA256, fuzzy hashing);

[36] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, *NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security*, 2015 (May), p. 247, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf., [6.03.2017].

[37] Ibid.

[38] S. Dai., Y. Fyodor, M. Wu, Y. Huang, S. Kuo, *Holography: a behavior based profiler for malware analysis*, „Software: Practice and Experience" 2011, Vol. 42, No. 9, pp. 1107–1136, http://dx.doi.org/10.1002/spe.1115.

[39] B. Genge, D.A. Rusu, P. Haller, *A connection pattern-based approach to detect network traffic anomalies in critical infrastructures*, [in:] *Proceedings of the Seventh European Workshop on System Security – EuroSec '14*, ACM, New York 2014, http://dx.doi.org/10.1145/2592791.2592792.

[40] E.D. Knapp, J.T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid*, *SCADA, and Other Industrial Control Systems,* Elsevier, Waltham 2015.

- Static analysis – such as checking if the malware code includes anti-virtual machine detection, anti-debugging (anti-reverse engineering) techniques and code obfuscation;
- Dynamic analysis – such as identification of network activities, system configuration/parameters modification, file activities;
- A hybrid approach – such as context aware classification.

The biggest challenge when dealing with advanced malware (like Stuxnet, Regin) is the malware's ability to bypass detection methods. Building variants; adding and including real garbage code and data; packing which requires special loaders; different encryption methods for code and data; obfuscation; detection of emulation/analysis/sandbox; using trusted/signed libraries and valid certificates; triggered activation (do not execute immediately); and detection of security products and processes in the running environment are the most common techniques among them. Malware will probably use the following techniques to avoid detection:

- Use zero-day vulnerabilities;
- Split the code and data into multiply files;
- Modify the malware code/data "on the fly";
- Modify the attack target "on the fly";
- Detect the memory scanning process;
- Detect the code analysis tool.

Malware, which is advanced enough to attack a smart meter, may disturb or influence the smart meter's important rules, like:

- Periodical power consumption registration;
- Private consumer activities;
- Communication with the utility company;
- The turning of the power on or off to any electronic devices which are connected to the local grid;
- Real time interaction awareness and management (e.g. load balancing);
- Automatic switching to an alternative power source like a solar, wind or alternative-energy storage system.

The malware may also eavesdrop on the home network traffic (which includes: pricing information, control structure, power usage, location information and private user data).

## Conclusion

The Smart Grid is an upgrade on the old electrical power grid and cyber security issues are a real threat. This has lead to the proliferation of industrial and academic research aimed at identifying and mitigating the cyber security threats which have been described in this paper. The paper serves as an overview and classification of the Smart Grid's cyber security challenges. From the cyber security perspective, the main challenge is the protection of the smart meter, which has been identified as the gateway between the HAN and the NAN, and is the critical point. The presented review of research in the field was focused mainly on advanced malware attacks on smart meters because advanced malware is the most dangerous threat to the smart meter itself. And because the smart meter is the gateway to the Smart Grid, advanced malware becomes a critical threat to the entire Smart Grid network, including but not limited to ICS (Industrial Control Systems) and critical infrastructures.

It is clear that adding encryption and cryptographic signatures to Smart Grid communication protocols is essential to ensure authenticity and integrity, but it will not solve the problem of advanced malware threats. For example, the unknown malicious codes, which are probably encrypted or use various programming obfuscation techniques, can bypass signature-based detection techniques.

The complexity and heterogeneity of the Smart Grid network means there will not be one golden solution, which addresses all cyber security threats. This makes Smart Grid protection in general and smart metering in particular a big research challenge and a very fruitful research field for the future.

For future research in the Smart Grid cyber security context, it is recommended that a new holistic approach is found that would be able to automatically build a malware baseline and the corresponding detection of malicious activities (for that reason Blockchain should be part of such a holistic approach). Future research should also investigate the use of a machine learning-based malware detection system. In particular, it would be interesting to combine machine learning with malware intrusion detection systems (IDS) specially built for Smart Grids.

## References

Ajayi A., Alese, B., Fadugba S., Owoeye K., *Sensing the Nation: Smart Grid's Risks and Vulnerabilities*, „International Journal of Communications, Network and System Sciences" 2014, Vol. 7, No. 5, pp. 151–163, http://dx.doi.org/10.4236/ijcns.2014.75017.

Baars T. et al., *Cyber Security in Smart Grid Substations*, Technical Report UU-CS-2012-017, Department of Information and Computing Sciences, Utrecht University, Utrecht 2012.

Baijusha R.J., Ganeshan R., *Cyber-physical system security using decoy system*, http://ijartet.com/.

Beasley C., Venayagamoorthy G.K., Brooks R., *Cyber Security Evaluation of Synchrophasors in a Power System*, Clemson University Power Systems Conference, Clemson 2014, pp. 1–5, http://dx.doi.org/10.1109/PSC.2014.6808100.

Bilge L., Dumitras, T., *Before We Knew It: an Empirical Study of Zero-Day Attacks in the Real World*, [in:] *Proceedings of the 2012 ACM Conference on Computer and Communications Security – CCS'12*, New York 2012, pp. 833–844, http://dx.doi.org/10.1145/2382196.2382284.

Chaffin M.N., *Common Cybersecurity Vulnerabilities in Industrial Control Systems*, U.S. Departament of Homeland Security, 2011.

Demme J. et al., *On the feasibility of online malware detection with performance counters*, [in:] *Proceedings of the 40th Annual International Symposium on Computer Architecture – ISCA '13*, ACM, New York 2013, pp. 559–570, http//dx.doi.org/10.1145/2485922.2485970.

Egele M., Scholte T., Kirda E., Kruegel Ch., *A survey on automated dynamic malware-analysis techniques and tools*, „ACM Computing Surveys (CSUR)" 2012, Vol. 44, No. 2, pp. 1–42 http://dx.doi.org/10.1145/2089125.2089126.

Egozcue E., Herreras Rodríguez D., Ortiz J.A., Villar V.F., Tarrafeta L., *Smart Grid Security. Annex I*, ENISA, 2012.

Fan X., Gong G., *Security Challenges in Smart-Grid Metering and Control Systems*, „Technology Innovation Management Review" 2013, Vol. 3, No. 7, pp. 42–49.

Gao Q., *Biometric authentication in Smart Grid*, 2012 International Energy and Sustainability Conference (IESC), Farmingdale 2012, http://dx.doi.org/10.1109/IESC.2012.6217197.

Genge B., Rusu D.A., Haller P., *A connection pattern-based approach to detect network traffic anomalies in critical infrastructures*, [in:] *Proceedings of the Seventh European Workshop on System Security – EuroSec'14*, ACM, New York 2014, http://dx.doi.org/10.1145/2592791.2592792.

*Guidelines for Smart Grid Cybersecurity*. *NISTIR 7628 Revision 1*., U.S. Department of Commerce, National Institute of Standards and Technology, 2014, http://dx.doi.org/10.6028/NIST.IR.7628r1.

Han C., Dongre R., *Q&A. What Motivates Cyber-Attackers?*, „Technology Innovation Management Review" 2014, Vol. 4, No. 10, pp. 40–43.

Hawk C., Kaushiva A., *Cybersecurity and the Smarter Grid*, „The Electricity Journal" 2014, Vol. 27, No. 8, pp. 84–95, http://dx.doi.org/10.1016/j.tej.2014.08.008.

He D. et al., *An enhanced public key infrastructure to secure smart grid wireless communication networks*, „*IEEE Network" 2014*, Vol. 28, No. 1, pp. 10–16, http://dx.doi.org/10.1109/MNET.2014.6724101.

Iyer S., *Cyber Security for Smart Grid , Cryptography , and Privacy*, „International Journal of Digital Multimedia Broadcasting" 2011, http://dx.doi.org/10.1155/2011/372020.

Jokar P., *Model-based Intrusion Detection for Home Area Networks in Smart Grids*, http://blogs.ubc.ca/computersecurity/files/2012/04/PJokar_HAN_IDS_-_Paria.pdf, [30.11.2014].

Knapp E.D., Langill J.T., *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid*, *SCADA, and Other Industrial Control Systems,* Elsevier, Waltham 2015.

Komninos N., Philippou E., Pitsillides, A., *Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures*, „IEEE Communications Surveys & Tutorials" 2014, Vol. 16, No. 4, pp. 1933–1954, http://dx.doi.org/10.1109/COMST.2014.2320093.

Lukas D., Kroustek J., Zemek, P., *Psyb0t Malware: A Step-by-Step Decompilation Case Study*, 2013, https://retdec.com/web/files/publications/DEC_WCRE_13.pdf.

*NCCIC/ICS-CERT Year in Review*, National Cybersecurity and Communications Integration Center/Industrial Control Systems Cyber Emergency Response Team, U.S. Departament of Homeland Security, 2015.

*NIST Framework and Roadmap for Smart Grid Interoperability Standards. Release 2.0*, National Institute of Standards and Technology, 2014, http://www.nist.gov/smartgrid/upload/NIST_Framework_Release_2-0_corr.pdf.

*NIST, 2009. NIST The Role of the Internet Protocol (IP) in AMI Networks for Smart Grid.*, p.16.

*Protecting Industrial Control Systems. Annex I*, ENISA, 2011.

Sato T. et al., *Smart Grid Standards: Specifications, Requirements, and Technologies*, Wiley, 2015.

Skopik F., Maa Z., Bleiera T., Grüneisb H., *A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures*, „International Journal of Smart Grid and Clean Energy" 2012, pp. 22–28, http://www.ijsgce.com/index.php?m=content&c=index&a=show&catid=27&id=16.

Skopik F., Smith P., *Secure Development Life Cycle*, [in:] *Smart Grid Security. Innovative Solutions for a Modernized Grid*, Elsevier, Waltham 2015.

Stelte B., Rodosek G.D., *Thwarting attacks on ZigBee – Removal of the KillerBee stinger*, [in:] *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*, Zurich 2013, pp. 219–226, http://dx.doi.org/10.1109/CNSM.2013.6727840.

Stouffer K., Pillitteri V., Lightman S., Abrams M., Hahn A., *Guide to Industrial Control Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)*, National Institute of Standards and Technology, U.S. Departament of Commerce, 2015, http://dx.doi.org/10.6028/NIST.SP.800-82r2.

*2016 Data Breach Investigations Report*, Verizon 2016, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

Wagner M., Kuba M., Oeder A., *Smart grid cyber security: A German perspective*, 2012 International Conference on Smart Grid Technology, Economics and Policies (SG-TEP), Nuremberg 2012, http://dx.doi.org/10.1109/SG-TEP.2012.6642389.

Wen H., Wang Y., Zhu X., Li J. Zhou L., *Physical layer assist authentication technique for smart meter system*, „IET Communications" 2013, Vol. 7, No. 3, pp. 189–197, http://dx.doi.org/10.1049/iet-com.2012.0300.

Zaddach J., Bruno L., Francillon A., *Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares*, https://www.internetsociety.org/sites/default/files/02_3_1.pdf.

The author is the Head of research cooperation with the industries at the Interdisciplinary Cyber Research Center (ICRC), Tel Aviv University, Israel and General Manager Cyber Security COE at Intel. He has been the CEO and Co-Founder of SCsquare Ltd., where he founded a business enabler for security technologies. He holds 16 approved patents in the area of cyber security. His career in cyber security over the past 20 years is a unique mixture of broad practical experience and research expertise. His practice included extensive involvement in cyber security offensive projects (software and hardware), business development and product management. Proven track records in secure operating systems, digital rights management, security certification, penetration test, reverses engineering, IoT security, ICS/Smart Grid security. The author is Ph.D. candidate at the Poznań University of Economics and Business, Poland. He holds a Masters of Business Administration (MBA) degree from Ben-Gurion University of the Negev, Israel.