Chapter 17
Cyber Security Objectives and Requirements for Smart Grid

Fernando Georgel Bîrleanu, Petre Anghelescu, Nicu Bizon and Emil Pricop

Abstract When we talk about smart grid we refer to the next generation of power systems that should and will replace existing power system grids through intelligent communication infrastructures, sensing technologies, advanced computing, smart meters, smart appliances, and renewable energy resources. Features of the smart grid must meet requirements as high efficiency, reliability, sustainability, flexibility, and market enabling. But, the growing dependency on information and communication technologies (ICT) with its applications and uses has led to new threats to discuss and to try to resist against them. On the one hand, the most important challenges for smart grid cyber security infrastructure are finding and designing optimum methods to secure communication networks between millions of inter-connected devices and entities throughout critical power facilities, especially by preventing attacks and defending against them with intelligent methods and systems in order to maintain our infrastructures resilient and without affecting their behavior and performances. On the other hand, another main challenge is to incorporate data security measures to the communication infrastructures and security protocols of the smart grid system keeping in mind the complexity of smart grid network and the specific cyber security threats and vulnerabilities. The basic concept of smart grid is to add control, monitoring, analysis, and the feature to communicate to the standard electrical system in order to reduce power consumption while achieving maximized throughput of the

F. G. Bîrleanu
Doctoral School of Faculty of Electronics, Telecommunications and Information Technology, University Politehnica of Bucharest, Bucharest, Romania
e-mail: birleanu.fernando@gmail.com

P. Anghelescu · N. Bizon (✉)
Faculty of Electronics, Communications and Computers, University of Pitesti, Pitesti, Romania
e-mail: nicubizon@yahoo.com

P. Anghelescu
e-mail: petreanghelescu@yahoo.com

E. Pricop
Department of Automatic Control, Computers and Electronics, Petroleum-Gas University of Ploiesti, Ploiesti, Romania
e-mail: emil.pricop@gmail.com

© Springer Nature Singapore Pte Ltd. 2019

E. Kabalci and Y. Kabalci (eds.), *Smart Grids and Their Communication Systems*, Energy Systems in Electrical Engineering,
https://doi.org/10.1007/978-981-13-1768-2_17

system. This technology, currently being developed around the world, will allow to use electricity as economically as possible for business and home user. The smart grid integrates various technical initiatives such as wide-area monitoring protection and control systems (WAMPAC) based on phasor measurement units (PMU), advanced metering infrastructure (AMI), demand response (DR), plug-in hybrid electric vehicles (PHEV), and large-scale renewable integration in the form of wind and solar generation. Therefore, this chapter is focused on two main ideas considering modern smart grid infrastructures. The first idea is focused on high-level security requirements and objectives for the smart grid, and the second idea is about innovative concepts and methods to secure these critical infrastructures. The main challenge in assuring the security of such infrastructures is to obtain a high level of resiliency (immunity from various types of attacks) and to maintain the performances of the protected system. This chapter is organized in seven parts as follows. The first part of this chapter is an introduction in smart grid related to how it was developed in the last decades and what are the issues of smart grid in terms of cyber security. The second part shows the architecture of a smart grid network with all its features and utilities. The third part refers to the cyber security area of smart grid network which involves challenges, requirements, features, and objectives to secure the smart grid. The fourth part of this chapter is about attacks performed against smart grid network that happens because the threats and vulnerabilities existing in the smart grid system. The fifth part refers to the methods and countermeasures used to avoid or to minimize effects of complex attacks. The sixth part of the chapter is dedicated to presenting an innovative methodology for security assessment based on vulnerability scanning and honeypots usage. The last part concludes the chapter and draws some goals for future research directions. The main purposes of this chapter are: to present smart grid network architecture with all its issues, complexities, and features, to explore known and future threats and vulnerabilities of smart grid technology, to show how a highly secured smart grid should look like and how this next generation of power system should act and recover against the increasing complexity of cyber-attacks.

Keywords Smart grid · Cyber security · Vulnerability · Reliability
Communication technologies · Threat · Attack · Countermeasure
Vulnerability assessment

17.1 Introduction

Smart grid refers to an evolved and efficient electricity grid system for a sustainable world and represents a junction between a classical electric network with all its features and utilities and ICT[1] elements that are meant to complement the grid functionality.

[1] Information and Communication Technologies.

"Grid" means everything used to provide electricity from the power plant for home and industrial use, such as transformers and transmission lines [1].

"Smart" indicates the two-way digital communication technology (client—supplier) and the sensing technologies through the translation circuit [1].

As a short history of making the conventional grid a "smart" one, the first known electric meter, using a simple electromagnetic to start and stop a clock, was licensed back in 1872 by Samuel Gardiner. Still, the data obtained from the electric meter were not enough because the indication referred only at the duration of the flow current and not the amount of it. After this, on December 20, 1879, Thomas Edison invented the incandescent light that is considered to be the ancestor of the modern light bulb that we use nowadays. Only three years later, at 3 o'clock in the afternoon on September 4, 1882, at the Pearl Street station, Thomas Edison expounded the first electric grid in lower Manhattan which illuminated either a red lamp or a blue lamp depending on the strength of the electromagnetic field in generators. In 1883, Hermann Aron invented a recording meter which was a better version of the first electric meter and which showed the energy used on a series of clock dials. In 1886, Edward Weston patented an indicating meter which was intended to measure current and not to measure consumption. This fact set higher standards when talking about precision. Only in 1889, the utilities were able to measure the amount of electricity provided to a customer thanks to Elihu Thomson who patented a recording wattmeter. The year 1970 was the beginning of meters which provided information back to the utility along with the apparition of the automatic meter reading devices. The technology for monitoring sensors and relaying the data grew out of the caller-ID technology patented by Theodore Paraskevakos [2, 3].

These old patents and technologies represent necessary fundaments for building the more efficient, reliable, scalable, and secure electricity distribution network that should become the smart grid [2, 3].

In Europe, the smart grid started in 2005 when the European Union established the European Technology Platform for the electricity networks of the future, or simply known as the smart grids platform that should be flexible, economic, reliable, and accessible with the 2020 goal for completing this [4].

In Canada, the Ontario's government initiated a program in 2006 where all consumers should receive smart meters by 2010 [4].

In Australia, in 2009, the government made a commitment to reserve $100 million for research and develop the smart grid with the objective to deliver a more robust and efficient energy [4].

Also in 2009, China's need for the intelligent grid led to the initiative called "Strengthened Smart Grid" made of three steps: planning and testing from 2009 through 2010, construction and development from 2011 through 2015, and upgrading from 2016 to 2020 [4].

The huge problem with the conventional energy system is that is low efficient at high and expanding costs, and it is expected that in 2030 the global electricity demand will increase with 75% facing the 2010 level of energy demand. The aim of smart grid is to incline the balance in the other way for very high efficiency at lower costs.

Money will be saved, outages will be reduced, new jobs will be available all this for a cleaner environment, higher reliability, and enforced worldwide economy [5].

Other issues of the smart grid, separated from efficiency and costs, is about the security of the smart grid network, the communication in the power grid network and about DSM,[2] also known as DSR[3] or simply energy demand management. Security is a huge test for designers of the smart grid because this new grid has challenges, vulnerabilities, and threats as many other systems have. The classic communication is based on serial communication which is predictable and reliable, while smart grid relies on broadband communication networks and nondeterministic communication environments. The goal of DSM is to strengthen consumers to use less amount of energy during peak hours or to move some electricity usage activities to different off-peak time intervals [6, 7].

Apart from these technical issues, there are some socioeconomic weaknesses such as the diminution of profitability on the generation and transmission segments of the system, conflicts of interest between industrial suppliers, and conflicts between national regulators and grid operators on charges and public service regulations [8–10].

It is supposed that with smart grid's yearly energy savings, a car can cruise 2.72 trillion kilometers enough for 70 million road trips around the world. Also, a refrigerator could run for 199 million years with the total energy saved in 1 year [11].

So, among the benefits that comes along with the smart grid, the most important are: better security, reduced costs for costumers, reduced management costs for suppliers, quicker restoration after disruptions, and increased efficiency for power transmission. Also, the customers will have their advantages. As already most of us manage some activities from home computer or smartphone such as home banking, think at how easy it will be to control electricity with a simple app with info's provided from a smart meter. Simply decide when and how power you use with real-time charges.

We agree that a smart grid network architecture will be very complicated involving a huge number of computers, sensors, controls, transmission lines, and so on. But if Internet already transformed our world and is part of how we live and work, why smart grid technology should not come up with similar changes in the near future?

17.2 Smart Grid Network Architecture

The three main components of the smart grid are the standard power grid, intelligent equipment, and communication infrastructure.

According to NIST,[4] ensuring the smart grid communications infrastructure requires five network sectors [12, 13]:

[2] Demand Side Management.

[3] Demand Side Response.

[4] National Institute of Standards and Technology.

- Enterprise bus—to connect control center applications to generators, markets, and each other;
- Field Area Networks—to control transformers and circuit fuses;
- Substation Networks—refers to premise networks in substations;
- Premises Networks—to connect utility premises and customers;
- AMI[5] Networks—to connect utilities to premises.

In order to meet expected goals, there is a series of technologies that smart grid combines which are as follows [4]:

- Integrated two-way communication

This technology empowers the operators for real-time interaction and monitoring of the smart Ggrid's components such as dealing more easily and at lower costs with outages. In classic grid, operators find out about disruptions only when customers notify them.

- State-of-the-art components

This technology allows to determine the electrical behavior of the grid and includes components as smart devices or diagnostic equipment for better energy management.

- State-of-the-art controls

This authorize operators to manage with smart grid controls for maintenance, diagnostics, and advanced data collection.

- Sensing and analyzing technologies

Sensing and analyzing technologies refers to sensors installed in each section of the grid used to detect and measure different parameters including security functionality, usage statistics, and smart grid stability. An important device of this section is the smart meter which monitors and sends electricity usage data to the utilities and to the consumers.

- Upgraded interfaces and determination support

This technology points in the direction of HMI[6] devices that must clarify data in a comprehensive and efficient manner so that operators proceed to verdicts very fast after interpreting what the machine analyzed.

- Applications technology

Applications will suggest to the customers recommendations for a reduced utility bill and also details about pricing, usage, and malfunctions all in real-time.

AMI viewed as the heart element of the smart grid consists of smart meters (SM), meter data management servers (MDMS), and data control units (DCUs) and will allow utilities to analyze, measure, and collect electricity usage stats from smart

[5] Advanced Metering Infrastructure.

[6] Human Machine Interface.

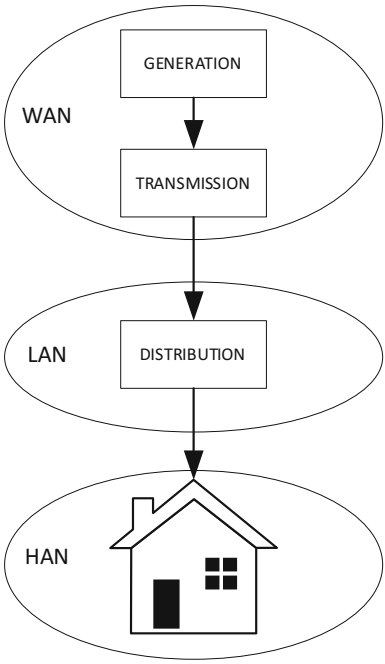

Fig. 17.1 Smart grid network hierarchical architecture

meters. For efficiency, the elements above will communicate using IP[7]-based network and to prevent data leakage and to have secured communications the devices will have to mutual authenticate [4, 6].

Viewed as a network of networks, the smart grid relies on a step by step hierarchical architecture, from the power plant to our homes, as detailed in Fig. 17.1. There are three networks: wide area network (WAN) for power plants, storage, and substations, local area network (LAN) for smart meters, gateways, and other elements in the distribution structure and home area network (HAN) for sensors and appliances [14].

A basic diagram for the smart grid's architecture is shown in Fig. 17.2. This basic diagram illustrates an intelligent power grid starting with the core, where the energy is generated. The energy flows to a transmission substation that is managed from a transmission control center. From the transmission substation, the energy flows to the distribution substations that are monitored from the distribution control center interrelated with the transmission control center. Distribution substations deliver the energy to the consumers where intelligent smart meters are installed. Through the smart meters, customers communicate wireless with the distribution center and vice versa for energy management using personal computers or smartphones in order to control home appliances or for energy consumption statistics [4].

NIST proposed a model architecture that contains seven logical domains: bulk generation, transmission, distribution, customer, markets, service provider, and oper-

[7] Internet Protocol.

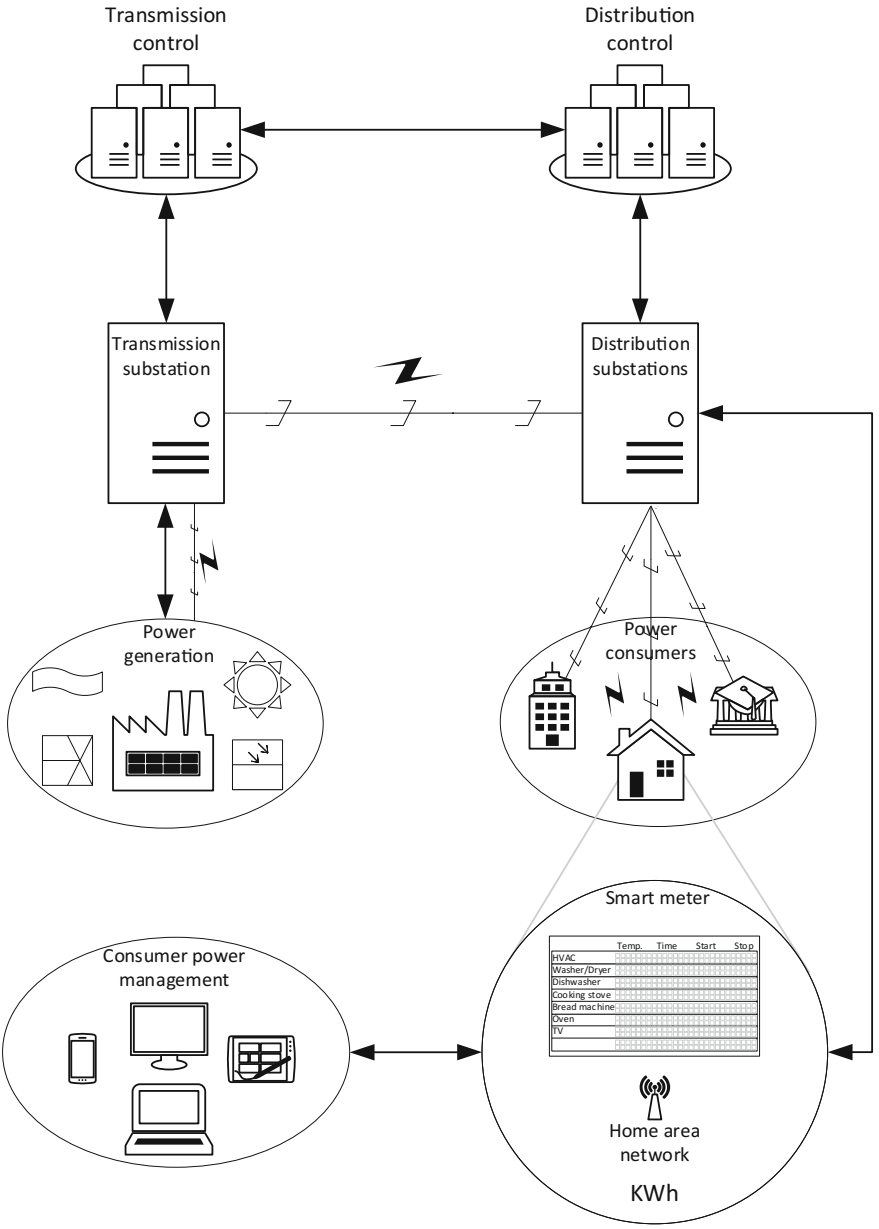

Fig. 17.2 A basic smart grid architecture

ations. From the bulk generation to the customer, it is detailed the two-way energy and information flows, while the last three domains highlight the smart grid's power management and information gathering. Figure 17.3 reveals an architecture for a

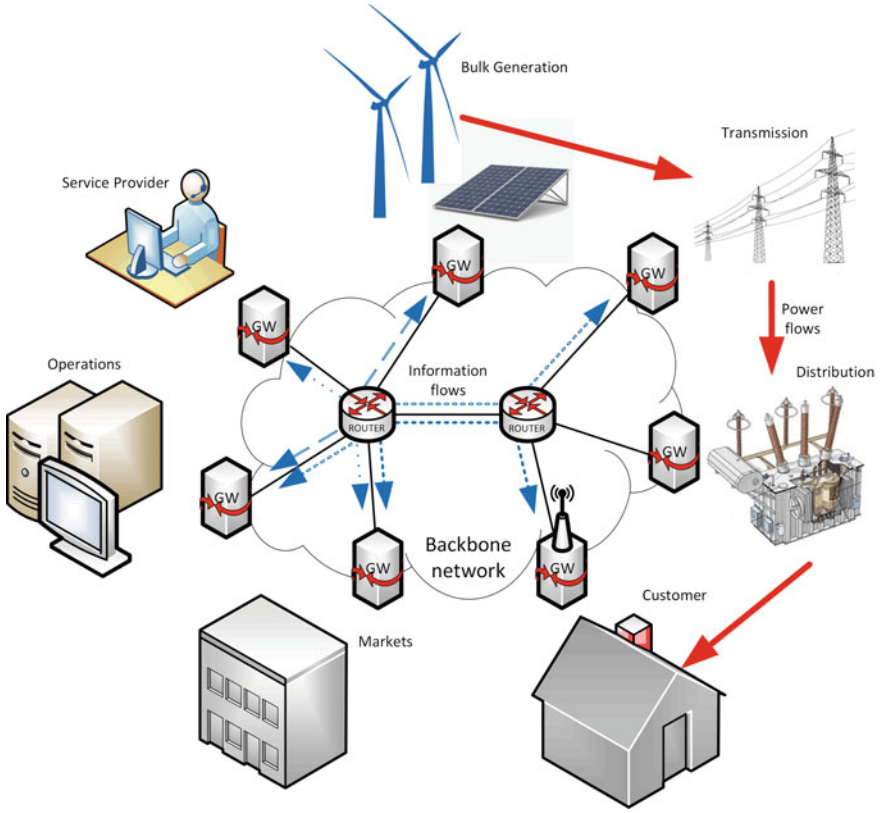

Fig. 17.3 NIST model for power network architecture

highly distributed and hierarchical smart grid network including the backbone network for inter-domain communication and local-area networks [13, 15, 16].

In Fig. 17.3, we can see how information flows between the logical domains. This communication infrastructure must meet some specifications in order to function as it is supposed to [17]:

- Real-time;
- Standards-based;
- Scalable;
- IP network;
- Increased availability
- Resilient;
- Mobile;
- Secure;
- Traffic prioritization platform;
- Lower costs.

Another architecture, depicted in [18] and called iCenS, was proposed at the 2016 IEEE International Conference on Smart Grid Communications. This architecture consists of three levels:

- Physical level—consumers, producers, and the infrastructure of power generation, transmission, and distribution;
- Aggregation level—information collector nodes for data gathering and operations controlling and monitoring;
- Computation level—cloud and data centers for statistical information, billing, and large-scale grid tracking and observation.

Main innovations that smart grid network architecture comes with are two-way communication, digital, sensors throughout, distributed generation, self-monitoring, self-healing, remote checking and testing and pervasive control versus old and still existing electric grid that is one-way communication, electromechanical, with few sensors, centralized generation, blind, manual repairing, manual checking and testing and limited control. Also, the consumers will dispose of many customer choices to evaluate their energy consumption and control intelligent appliances [14].

So, a smart grid network must satisfy features such as resilient, efficient, intelligent, load handling, and green, but the architectures above have certain cyber security goals and requirements and without them building such an intelligent network would not be possible [19].

17.3 Cyber Security—Objectives and Requirements for Smart Grid

There are multiple upgrades that smart grid is intended to achieve that are based on innovative technologies and on the collaboration of different organizations. Among these improvements arise the easy access to devices and power data problem that directs to existing and new attacks to be performed against the intelligent grid. We are aware that fully secured systems and apps do not exist and that smart grid technology will not be by-passed [4].

NIST released three high-level cyber security objectives (Fig. 17.4) that are [16, 20, 21]:

- Availability—ensures that services and information are timely and reliable accessed by its users and must prevent attacks against utility companies and consumers;
- Integrity—ensures information authenticity and non-repudiation against modification or destruction attacks that can lead to inappropriate judgement for energy administration;
- Confidentiality—ensures information defense against unauthorized access or disclosure.

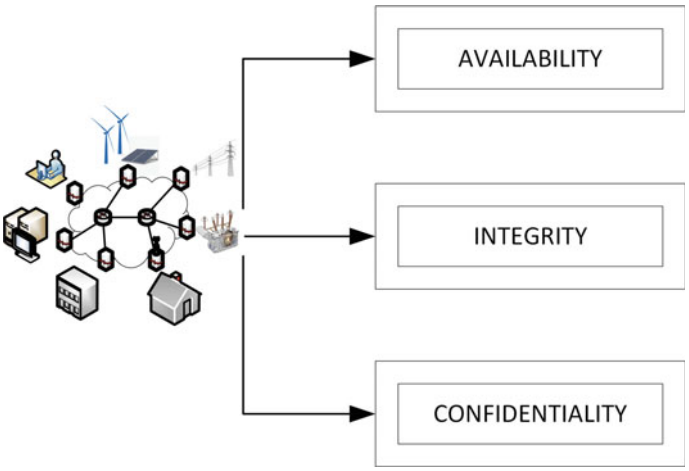

Fig. 17.4 NIST three high-level cyber security objectives

The first two objectives are the most critical and important in the smart grid network from a reliability point of view, while the least crucial, confidentiality, is getting more and more essential in the HAN on the communication with the customers and in systems such as AMI networks [16].

Cyber security requirements for the smart grid, also recommended by NIST, involves physical security and cyber security that deal with critical parts such as communication or smart endpoints. These requirements are [16]:

- Highly secured and efficient communication protocols;
- High resiliency and attack recognition;
- Access control, identification, and authentication.

In terms of security, the eye is on the HAN security because customer's privacy is a crucial point and LAN's and WAN's security are in a very wide range discussed. Usually, a HAN consists of four items: a gateway to connect HAN with services in the LAN or WAN, network nodes or access points, a software management and operating system for the network and smart endpoints (smart meters, appliances or info displays) [14].

As an example, Fig. 17.5 shows the main particularities such as security algorithm (AES,[8] DES,[9]) radio frequency band, and bit rate for wireless network standards to implement a HAN [14]. The customer's biggest concern refers to data protection exchanged between the utility company and the smart meter.

In [22] are described some security challenges in the transition to an intelligent grid as below:

- The challenge in ensuring customer security;

[8] Advanced Encryption Standard.

[9] Data Encryption Standard.

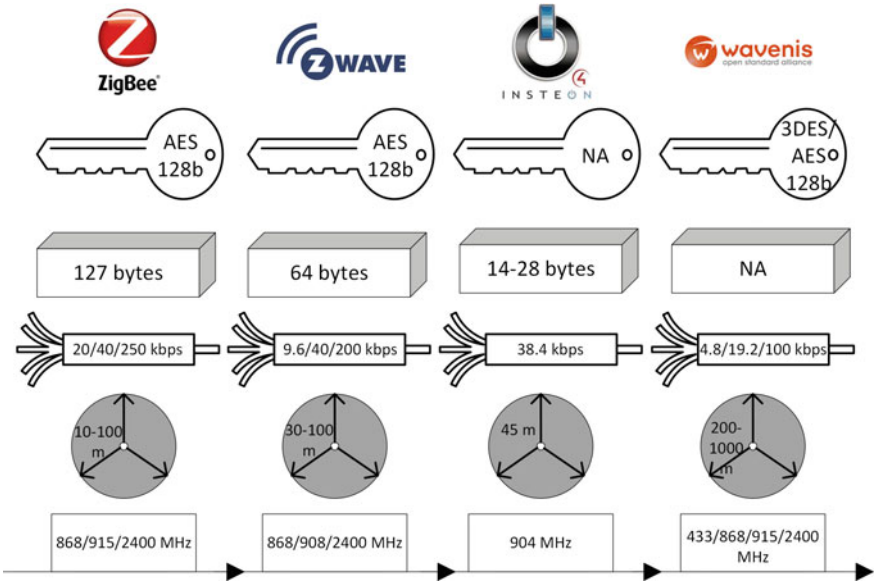

Fig. 17.5 HAN standards and characteristics

- The challenge of handling with the problem of physical security;
- The challenge in dealing with a huge number of devices;
- The challenge in dealing with more stakeholders;
- The challenge in the use of IP and commercial of the shelf hardware and software.

Under these circumstances, it is obvious that new techniques and technologies are needed in order to increase the cyber security of the smart grid. As more and more distributed information needs to be processed and protected, artificial intelligence techniques based on cellular automata, genetic algorithms, fuzzy logic, and artificial neural networks provide new solutions through local interconnections. As an example, information protection systems based on cellular automata offers, in some cases, new opportunities for the smart grid domain that can be used in conjunction with traditional security solutions [23–25].

In line with the features, objectives, requirements, challenges, and advantages that future smart grid must come with are the attacks that are performed by hackers either for financial gains or others advantages [26].

17.4 Attacks Against Smart Grid

Attacks against the smart grid network start by detailing the potential risks and threats that the grid must deal with. For the smart grid, the main potential risks and threats are [14, 27–30]:

- New technologies can bring new issues in the network;
- The grid is too complex, and this can lead to weak points or unforced errors;
- Intelligent nodes can contribute to denial-of-service (DoS) attacks;
- There are many network links that can compromise the entire system;
- Interference with utility telecommunications that can alter the generation, transmission, and distribution system;
- Bill manipulation for energy theft;
- Unauthorized access from customer end device or point;
- Manipulation of mass load in order to disturb the bulk power grid;
- Equipment failure;
- Human errors;
- Threats that happens naturally because of the weather, fire, or animals.

In general, an attack has four steps:

- Investigation;
- Discovery;
- Vulnerability identification;
- Infiltration.

There is a large variety of attacks against smart grid and many ways to categorize them depending on technologies used, layers, platforms, and so on. Here there are four aspects to consider: attacks based on smart grid security objectives, attacks against the utility companies, attacks against the customers, and attacks regarding wide-area monitoring, protection and control systems (WAMPAC). WAMPAC is a technology based on PMUs that ensures real-time monitor current grid operations and real-time protection and control activities such as automatic generation control (AGC) and special protection schemes (SPS) [31, 29, 30].

Attacks based on the three high-level cyber security objectives are [16]:

- Attacks that point availability—these attacks are the DoS attacks (jamming in substations, ARP[10] spoofing, traffic flooding, buffer flooding) that are intended to corrupt, block or to insert delays in the communication inside smart grid;
- Attacks that point integrity—these attacks are designed to disrupt or to modify data traffic inside the smart grid network such as false data injection, net metering, and sensor data manipulation;
- Attacks that point confidentiality—these attacks look for collecting unauthorized data and information from network capabilities in the intelligent grid such as traffic analyzing and eavesdropping.

[10] Address Resolution Protocol.

When attacking the utility companies, usually, hackers use multiple attack schemes on several parts and resources of the utility organization in order to achieve their goals. Thus, attacks against the utility companies are separated as [4]:

- Physical attacks;
- Network attacks;
- System attacks;
- Wireless attacks;
- Application attacks;
- Social engineering attacks.

When attacking customers hackers perform attacks against HAN. These attacks include [4]:

- Network attacks;
- Wireless attacks;
- Attacks against smart meters;
- Attacks against management devices.

Cyber-attacks against WAMPAC in smart grid are divided in three parts [31, 32]:

- Replay attacks—through these attacks hackers manipulate the PMU by stealing transit packets;
- Timing attacks—these attacks are intended to the communication network with packets to slow down or to shut down the network;
- Data integrity attacks—these attacks corrupt data in the forward or reverse path in the control flow.

Because one of the biggest problems in power systems is the disturbance event, either as a result of an attack or as a result of natural disasters or effects, Fig. 17.6 shows an approach for disturbance event classification considering the most frequently events occurred in a power system. This event classification precedes methods for event detection and location and for countermeasure mechanisms against attacks [33, 34].

17.5 Countermeasures for Attacks Against Smart Grid

Countermeasures methods are detection and defense mechanisms to protect against malicious attacks and without them the smart grid could not become reality.

In the previous section, we talked about attacks based on the three high-level cyber security objectives. These can be prevented with a series of countermeasures [14]:

- For attacks targeting availability, it is used the redundancy technique;
- For attacks targeting integrity countermeasures are based on access control, where only authorized users can come up with modifications;
- For attacks targeting confidentiality, it is used the least privilege principle, where a user has the exact needed privileges to implement his actions.

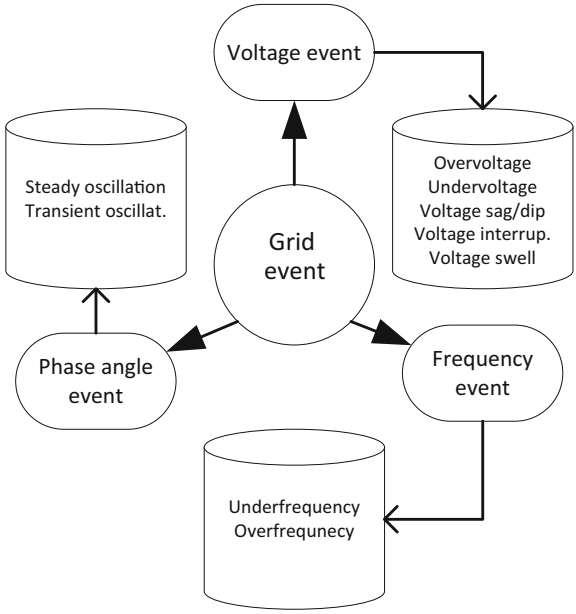

Fig. 17.6 Disturbance event classification

But, the point with these countermeasures is to cover the entire smart grid and not only high-level cyber security objectives. Thus, the next countermeasures refer to defense mechanisms to protect the power network of the smart grid, at cryptographic methods to secure communication in the network and at security practices to secure the consumer and the utility companies.

For the power network in the smart grid, there are two countermeasures methods [16]:

- Attack detection with four mechanisms: packet-based detection, signal-based detection, proactive method (algorithms based on sending probing packets), and hybrid method (a combination between the other three methods or other existing methods);
- Attack attenuation with three mechanisms: reconfiguration of the network architecture, rate-limiting on possibly malicious set of packets and packet filtering after attack detection.

Cryptographic mechanisms for the smart grid network communication are major countermeasures against attacks and more effective than the power network approaches. These mechanisms include [16, 35]:

- Encryption based on symmetric key cryptography (AES, DES);
- Encryption based on asymmetric key cryptography (RSA[11]);
- Authentication;

[11] named after Ron **R**ivest, Adi **S**hamir, and Len **A**dleman, who invented it in 1977.

- Key management (PKI[12] and symmetric key management).

Countermeasures methods to secure a customer and its HAN of a smart grid can be encapsulated in a 12 steps security practice as those that follows [14]:

Step 1. Threat modeling—potential threats must be found in order to implement countermeasures;
Step 2. Segmentation—minimize the impact and surface of attacks;
Step 3. Firewall rules—convenient rules must be utilized;
Step 4. Signing—digital signing for trusted applications in the grid;
Step 5. Honeypots—traps for hackers so that alerts come in time;
Step 6. Encryption—protecting sensitive data and information;
Step 7. Vulnerability analysis—centers for analyzing traffic and critical systems;
Step 8. Penetration testing—simulation of attacks to observe how efficient are countermeasures;
Step 9. Source code review—the applications in the intelligent grid must present zero vulnerabilities;
Step 10. Configuration hardening—vulnerabilities scanner and benchmarking test, especially for smart endpoints;
Step 11. Strong authentication—at least two-factor authentication;
Step 12. Logging and monitoring—provides information for attacks identification and for reassemble actions in case of natural failures.

Also, in the same way, there is a 12 sections security practice for securing the other end of the smart grid—utility companies which represents the ISO/IEC 27002—Code of Practice for Information Security Management [4]:

Step 1. Risk assessment—for identification and prioritization of the risks against the information grid;
Step 2. Security policy—to direct and evaluate the information security plans of the utility companies;
Step 3. Organization of information security—it is an important factor in the successful and correct implementation of a functional information security plan;
Step 4. Asset management—to identify who is responsible for particular assets;
Step 5. Human resources security—refers to the information dissemination to the contractors or staff who must assume their responsibility regarding the security of the information that they just acquired;
Step 6. Physical and environment security—this section is about protecting critical systems of the grid and preventing unauthorized access;
Step 7. Communications and operations management—someone must be an accountable and must respond for grid's information systems;
Step 8. Access control—least privilege principle;

[12]Public Key Infrastructure.

Step 9. Information systems acquisition, development, and maintenance—utility companies must ensure that all information security requirements are included while a project is in the requirements step;
Step 10. Information security incident management—refers to those methods implemented for the timely identification and containment of information security incidents;
Step 11. Business continuity management—utility companies must hold up incidents that affected the continuity of their operations and actions;
Step 12. Compliance—standards and legal requirements.

All this countermeasures for attacks against smart grid are meant to prevent and to protect the entire power network in case of intrusions, to alert and to take action for combating these actions.

17.6 Assessing the Vulnerabilities Associated with Smart Grid Components and Their Potential Impact

The previous sections of this chapter offer an overview on the security issues associated with smart grids. The main types of attacks that could occur on smart grid and corresponding countermeasures were briefly described. The main challenge is to assess the security state of a given system by manual or automatic means.

In this section, the authors will present an automated method for assessing the vulnerabilities of a networked system. The basic functioning of a vulnerability scanner will be described next.

17.6.1 Vulnerability Scanners

Security risks assessment is a very challenging task since the threat landscape is very dynamic. In order to obtain a complete image, it is necessary to have information regarding three factors:

1. the number and severity of the system's vulnerabilities;
2. the attacker interest in the systems;
3. the existing security measures.

The vulnerability assessment can be realized by two different methods:

- manual testing using the so-called pentesting technique;
- automated testing by using a specialized software.

Pentesting consist in hiring an experienced attacker, known as *ethical hacker*, for trying to compromise the target system by various methods and techniques including social engineering, exploiting known vulnerabilities and initiating attacks. When the

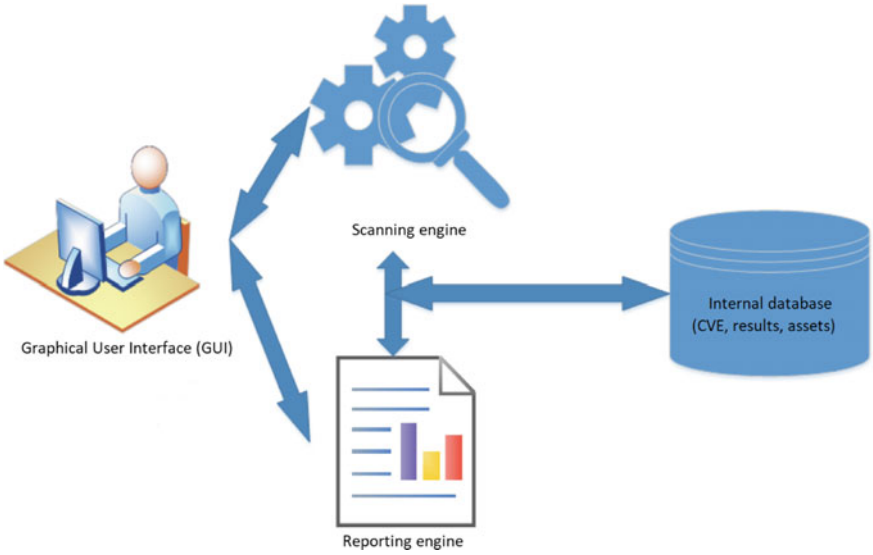

Fig. 17.7 Structure of a generic vulnerability scanner [36]

testing period finishes, the attacker should provide a report that contains all the discovered breaches and methods for fixing them.

As presented in reference [36], the pentesting activity presents some major security risks as shown below:

- exposing vulnerabilities of the tested system in various online environments (forums, social networking sites, etc.), making them available for potential attackers who could not otherwise identify them;
- exposing confidential data about the architecture of the tested network, existing security measures, account validation procedures, etc.
- identifying vulnerabilities that will not be presented to the beneficiary, but which could be used either for blackmailing the beneficiary or to sell them to the competition.

The risks mentioned above are very sensitive for a business. If the network of a smart grid operator is tested by a so-called ethical hacker, and some vulnerabilities are discovered and published directly to the media, this issue can have a significant impact on the image and trust on the operator.

In the opinion of the authors, the automatic test method does not pose the same security risks. The method consists of using a software package named vulnerability scanner.

A generic *vulnerability scanner* has a modular structure as presented in Fig. 17.7.

The vulnerability scanner should include at least the following modules [36]:

- internal database;

- the scanning engine;
- reporting engine;
- user interface.

There are two critical components for the functioning of the vulnerability scanner. The first one is the internal database which stores the vulnerabilities "definitions", representing their formal description, the method that should be used to identify them, their impact and methods to protect the system against them.

Often the **internal database** is a replica or is directly connected to an CVE—Common Vulnerabilities and Exposures directory. The MITRE CVE Database [37], available online on http://cve.mitre.org, is listing a large number of vulnerabilities that affect industrial systems.

The CVE database records are identified by a unique name formatted as CVE-YYYY-NO_ID, where YYYY represents the year of vulnerability discovery and NO_ID is a unique serial number allocated to the vulnerability. The serial number NO_ID reset every year.

Each CVE record should contain at least three fields, as described below:

- *description* is a text field that contains a brief description of the vulnerability and the possible impact on given systems;
- *references* is a blob (large text) field of high importance since it contains links to pages that present detailed characterization of vulnerability. The information stored in this field will point the user to detailed description of the vulnerability, known protection methods and patches;
- *record date* shows the calendar date when the vulnerability was added to the CVE database. This date does not indicate exactly when the vulnerability was identified, since each equipment (software or hardware) producer may take some time to release a fix for an identified vulnerability.

A sample CVE record is shown in Fig. 17.8. In the upper part of the image, it is displayed the unique vulnerability identifier (CVE-2008-4827), and in the lower part, the links to vulnerability details are listed.

In the author opinion, the CVE list can be considered a unique vulnerability identification and description language, since the large majority of security solutions use this notation for describing security issues.

The **scanning engine** is the kernel of the vulnerability scanner, and it performs the verification process of each protected object using a specific algorithm that should contain the steps shown in Fig. 17.9.

The first step of the algorithm is to identify the active systems in the network. In this step, the scan engine checks the presence of hosts on the network using their IP address and sending ICMP[13] Echo Request messages. If a host in the network receives such a message, it will respond with ICMP echo reply, which will indicate that the device is active and can transmit data to the network [36].

[13] Internet Control Message Protocol.

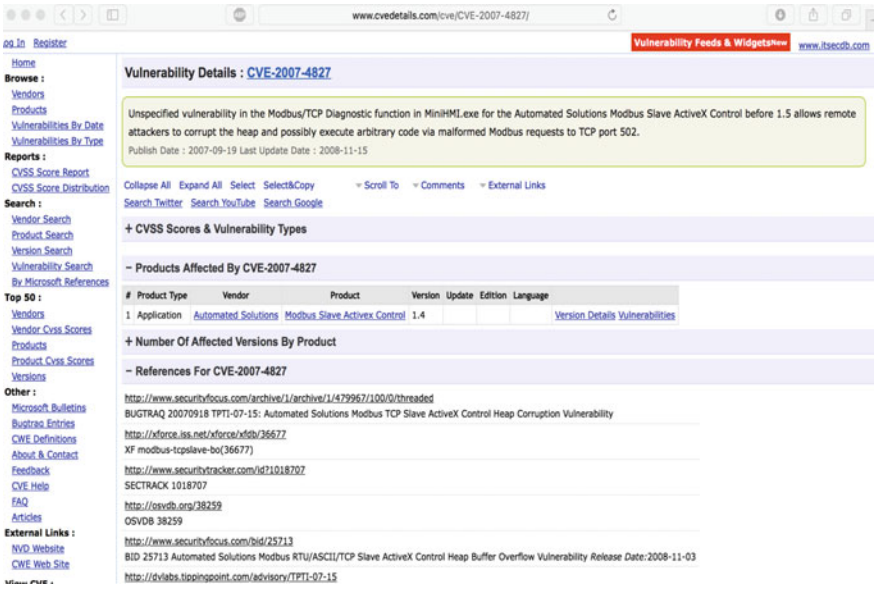

Fig. 17.8 Example of CVE record [37]

The next step of the algorithm involves detecting open TCP[14]/UDP[15] ports on each identified active device. One of the simplest detection methods is to try to connect on ports from a predefined list (most used ports are well-known) or to probe all ports in the range 0–65535. If a connection can be established on that port, then it is considered open.

The third step of the algorithm is to determine the services offered by the scanned equipment on each active port. Some TCP and UDP ports are assigned to standard applications, such as 80—HTTP,[16] 21—FTP[17] or 25—SMTP[18] and the scanner might assume that the standard service is operated on the port, if it is found open. Confirmation of service type can be then done by the scanner by interpreting and analyzing the received responses to queries specific to the type of searched protocol.

The last steps of the algorithm allow for direct identification of existing vulnerabilities. Based on the port and service information available on each host, the scanner will launch a fingerprinting operation for each service and port. This type of operation automatically interprets and analyzes the response of each application to a specific query. Following the steps described above, the vulnerability scanner will determine for each analyzed host what operating system is installed, the type and version of

[14] Transmission Control Protocol.

[15] User Datagram Protocol.

[16] HTTP—Hyper-Text Transfer Protocol.

[17] FTP—File Transfer Protocol.

[18] SMTP—Simple Mail Transfer Protocol.

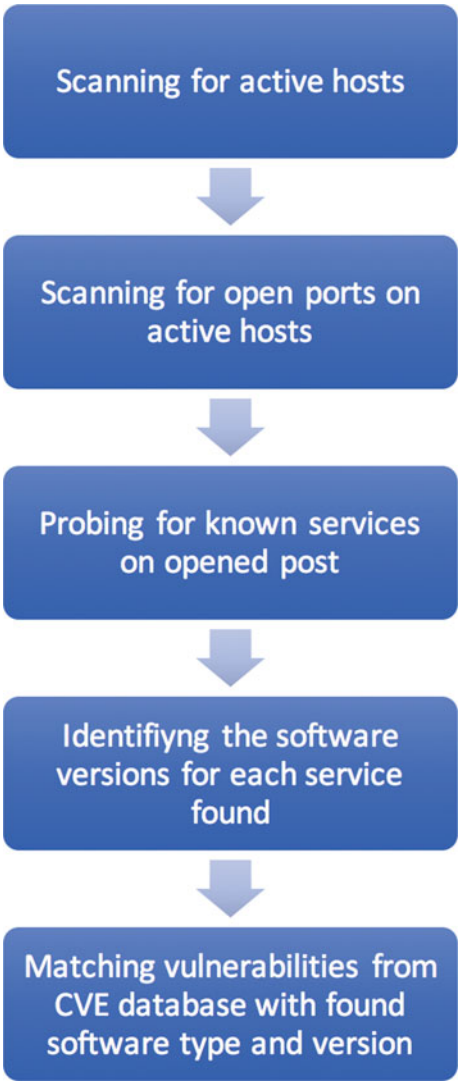

Fig. 17.9 Basic algorithm for vulnerability scanner operation [36]

the running applications, and whether they can connect to them. Based on this information, the scanner searches the internal database and lists the vulnerabilities of the detected system and applications.

The **user interface** is the component of the vulnerability scanner that allows user interaction. Most of these scanners feature an intuitive and very user-friendly graphical interface. In most cases, this interface is a Web page that contains well-documented graphics and buttons that allow the user to focus on identifying security issues. Examples of such programs are: Nexpose [38] or OpenVAS [39]. However,

there are also vulnerability scanners with command line interface, such as Nmap [40] or Nessus [41]. Although they are highly performing, such scanners are more difficult to use by people less familiar with the use of command line (text based) interfaces.

The fourth module of a vulnerability scanner is the **reporting engine.** It is used to automatically generate scan reports that can be customized to include more or less information according to the beneficiary profile. For example, if the report is addressed to a developer or system administrator, it should contain detailed descriptions of the vulnerabilities found and suggestions for fixing them. In the same time, if the report will be presented to the company management, it will present only a global threat assessment.

The vulnerability scan result can be presented as a numeric index or as a semantic value that shows the level and potential impact of detected security problems. Unfortunately, the index is based only on known vulnerabilities that are already published in specific databases. It is obvious that smart grid systems might be affected by undetected vulnerabilities and breaches such as buffer overflows or software bugs that can be exploited by experienced attackers.

17.6.2 Honeypots—Concept and Classification

The likelihood and the success of a given attack does not depend only on vulnerabilities level, but as shown in references [36, 42–45] on attacker interest and abilities and on countermeasures taken to protect the system.

The usage of honeypots for industrial systems such as smart grid is a recent idea that can provide an accurate image regarding the interest of attackers and the attack methods.

In the following paragraphs, we will introduce the honeypot concept and we will present the general characteristics of these systems.

A honeypot is a networking resource that can be tested, attacked, or compromised without causing damage. Basically, a honeypot is a trapping mechanism that can be used for research purposes to test communications protocols that are often targets of computer attacks and to assess how to initiate and run an attack, or can be false targets for an attacker.

According to [46], a honeypot is a system configured to be exposed to the Internet for potential attackers, to attract them through the distribution of supposedly valuable information. When the system is accessed, it must record each of the attacker's actions within protected log files. It is very important to mention that the compromise of the system must not cause any damage to other network components or even to other networks.

The resulting log files can be used to accomplish the main function of a honeypot system, namely the analysis of the source and attack mechanisms. The log files can provide various information about the attacker, such as the IP address, the operating system used, the geographic location with greater or lesser accuracy. Some honeypot

systems allow recording all of the commands/steps followed by the attackers, creating a real modus operandi for each attack. Another important characteristic of honeypot systems is the ability to get information about new vulnerabilities or new ways to exploit existing vulnerabilities.

In order to characterize the honeypot operation, the interaction level concept should be defined. This concept represents the degree of interactivity of the system with the user, and the extent to which an attacker can run commands on the system and receive a feedback from it [47]. This factor also indicates the functionality of the honeypot.

The more higher degree of interaction a honeypot has, the greater is the amount of information it can gather. At the same time that the risk of the honeypot to be hijacked by the attacker and used to launch new attacks, usually within a botnet, is also increased.

From the point of view of the interaction level, honeypots can be categorized into two categories [36]:

- **LIH**[19] is currently the most widespread, due to their lower complexity and less resources. Such systems emulate certain services that are tempting for attackers. The activities that may be deployed by the attacker are limited and can be summarized as a contact attempt or just listing the contents of a directory on an FTP server.

LIHs are often configured so that the attacker attempts to block the attack, it is disconnected, thus eliminating the risk of penetration of the system and its use by the attacker to launch other attacks. Due to the fact that LIH allows the execution of a limited number of predetermined actions, the information gathered is limited. Typically, IP data, geographic location, operating system, and software used by the attacker are usually obtained, but no information can be obtained about how a particular type of attack is taking place.

- **HIH**[20] is very complex. Such systems do not just simulate the existence of a particular network service, but replicate the entire operation of this service. Practically, when an attacker accesses a HIH, he can use simulated services and can launch commands without realizing that he is actually using a trap system.
- HIH poses a high-security risk and therefore needs permanent monitoring because an experienced attacker can take control of the machine and can use it to launch various attacks on other targets.

Reference [47] shows a classification of honeypots according to where they are located in the network and data management mode, with three generations of honeypots highlighted.

[19] Low Interaction Honeypot.

[20] High Interaction Honeypot.

17.6.3 Industrial Honeypots Examples

The honeypots were first developed and deployed in order to test the security of Web applications. They were used to replicate common services such as HTTP servers. In the last decade, there were developed some honeypots dedicated to industrial protocols. In this section, we will briefly present the characteristics of three open-source solutions for industrial level honeypots, namely *ConPot, Dionaea,* and *Cowrie.*

ConPot [48] is an open-source honeypot developed by Honeynet Project [49], designed to emulate industrial networking protocols and automation devices such as programmable logical controllers and frequency converters. It is a LIH that offers the ability to emulate various industrial protocols, including Modbus/TCP, for field-to-field communication and PLCs,[21] and S7Comm, a protocol developed by Siemens for communication between PLCs from Step7 family, some of the most used controllers in the industrial environment. ConPot can also create a simple human–machine interface that can be delivered as a Web page through the HTTP protocol on the 80 TCP port.

Dionaea [50] is one of the most commonly used honeypot systems. It was developed on the basis of the Nepenthes project within the 2009 Summer of Code Honeynet Project. Dionaea seeks not only to create a simple trap for attackers, but also to develop a mechanism for capturing malware used to exploit simulated vulnerabilities.

Dionaea has a complex architecture. It was written using the Python programming language. By default, Dionaea can be used to simulate the communication protocols outlined below:

- **SMB**[22]—is the main protocol simulated by Dionaea. SMB runs on TCP ports 137, 139 and 445 and on UDP ports 137 and 138 that are being used for inter-process communication as well as for accessing shared resources on the network;
- **HTTP and HTTPS,** using TCP ports 80 and 443, respectively, are used to transfer Web pages;
- **FTP**—is specific to TCP port 21. The FTP protocol is used for file transfer. Dionaea implements an FTP server that allows creating new directories, uploading and downloading files, making this protocol a honeypot with a high degree of interaction but with a more limited number of commands than a real server;
- **Trivial File Transfer Protocol** runs on port 60 and can be accessed by the attacker for downloading files.

Cowrie [51] is a HIH developed by Michel Oosterhof. The purpose of the honeypot is to simulate a SSH[23] server, to log login and password enrollment attempts, and for successful login attempts to record all attacker actions on the server. Cowrie allows the running of a large number of SSH protocol-specific commands, and the latest releases are implementing Diffie–Hellman encryption key exchange mechanisms and even the ability to make secure SFTP connections.

---

[21] Programmable logic controller.

[22] Server Message Block.

[23] Secure Shell.

The SSH protocol, although not an industry-specific protocol, is commonly used in embedded systems (wireless sensors, data concentrators) that run a Linux kernel and can be configured remotely. For this reason, the data provided by the Cowrie honeypot are valuable for analyzing attacks in the industrial environment.

17.6.4 Results Obtained Using Industrial Honeypot—ConPot

For assessing the interest of attackers on industrial systems the authors installed the ConPot honeypot, specific to emulation of industrial systems as presented in the previous section.

The honeypot was configured to run the following protocols:

- Modbus/TCP on TCP port 502;
- S7Comm on TCP port 102;
- HTTP on TCP port 80;
- SNMP[24] on TCP port 161;
- IPMI on TCP port 623.

SNMP is a client-server protocol used to obtain status and configuration information for networking equipment. The client can send requests to any device compatible with SNMP and the device will answer with state or configuration information. This protocol is critical for network security since it can expose the configuration of key network component making the whole infrastructure vulnerable to attacks.

IPMI[25] is a protocol generally implemented by server manufacturers for remote management, independent of the existing operating system or server status. IPMI can monitor hardware parameters, but server shutdown or restart commands can also be sent [36].

The services mentioned above are simulated, so they only allow an attacker to connect but does not allow him to run commands. Conceptually, Conpot opens the specified TCP ports for connecting the attacker, and when making a connection, it records all available connection source information: event date and time, source IP address, client type if available and then closes the connection. Taking into account that the honeypot does not allow commands to run on any of the simulated protocols, the attacker can detect the trap in a very short time. Therefore, it is necessary to periodically change the IP address used.

Table 17.1 is showing the centralized results obtained by using ConPot for one week in September 25, 2017–1 October 2017 on a virtual private server located in a commercial hosting provider datacenter. The server was running Ubuntu Linux operating system and was directly connected to the Internet, without using any kind of hardware or software firewall.

[24] Simple Network Management Protocol.

[25] Intelligent Platform Management Interface.

Table 17.1 Results after using ConPot for one week

Protocol type	Total connections/protocol
HTTP	48
SNMP	39
MODBUS	17
S7Comm	14
IPMI	9
Total	38

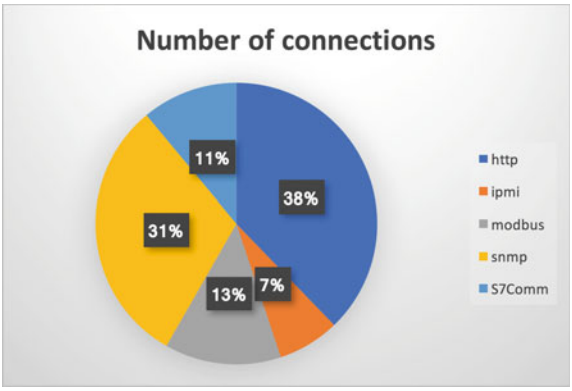

Fig. 17.10 Distribution of attack attempts by protocol type

The chart in Fig. 17.10 is showing the distribution of the connections (attack attempts) by protocol type.

It is obvious that the most targeted protocol is HTTP, which is tempting for all attacker types and is exploited even by automated software instruments.

31% of the connections registered were made using SNMP protocol. As mentioned in the previous section, this protocol may disclose valuable networking information that can be used in phase of discovery attack and then might be exploited in an access cyberattack.

Modbus/TCP (13%) and S7Comm (11%) are targeted by a concerning number of attack attempts. 24% of the total connections (approximately 1 out of 4 connections) are made on specific TCP ports for industrial protocols. This situation indicates an increased interest in accessing the industrial infrastructures that are connected to the Internet such as smart grids.

The data obtained by using ConPot confirm the interest of attackers on industrial protocols. Also, it shows that the network administrator should ensure a good security level on the targeted ports (502—Modbus and 102—S7Comm).

Data obtained from honeypot systems show the attacker interest on a given system. Our future research will focus on creating a HIH that will replicate networking components of smart grids. By using such a honeypot, the administrator will be able to identify the most targeted systems and to harden their security.

17.7 Conclusions

Smart grid is supposed to create a complex intelligent electric grid network with increased efficiency, high resiliency, and many other benefits. Due to its high architectural complexity and critical requirements and challenges, the main goal in creating the next-generation power grid is to achieve high-level cyber security against existing attacks and many other complex attacks that appear once with the implementation of new and innovative techniques and technologies into the smart grid. This security can be achieved only by implementing efficient countermeasures against attacks through ingenious methods and mechanisms with resistance, evidence, detection, and response functions in order to maintain the system's availability, integrity, and confidentiality.

In the previous sections, the authors presented an overview of smart grid security and the concepts of using vulnerability scanners and honeypot for evaluating the actual security level and the attackers' interest in industrial systems.

The general conclusion of this work is that in the near future smart grid networks will become functional through different ICT infrastructures for a more reliable and secure energy system.

References

1. https://goo.gl/xn37xa
2. https://goo.gl/xvnPAc
3. https://goo.gl/LtNfWN
4. T. Flick, J. *Morehouse, Securing the Smart Grid—Next Generation Power Grid Security* (Syngress, 2011)
5. https://goo.gl/SkNCpD
6. https://goo.gl/nn22ET
7. https://goo.gl/dgSnkT
8. A.V. Gheorghe, M. Masera, M. Wiejnen, L. De Vries, *Critical Infrastructures at Risk* (Springer, 2006)
9. K. Pipyros, C. Thraskias, L. Mitrou, D. Gritzalis, T. Apostolopoulus, A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual. Comput. Secur. (2017)
10. B. Karabacak, S.O. Yildirim, N. Baykal, Regulatory approaches for cyber security of critical infrastructures: the case of Turkey. Comput. Law Secur. Rev. **32**, 526–539 (2016)
11. https://goo.gl/aZ4cSb
12. https://goo.gl/dx3855
13. https://goo.gl/38rpxU
14. https://goo.gl/chTezx
15. Office of the National Coordinator for Smart Grid Interoperability, NIST framework and roadmap for smart grid interoperability standards, release 1.0, NIST Special Publication 1108, 1–145 (2010)
16. W. Wang, Z. Lu, Cyber security in the smart grid: survey and challenges. Comput. Netw. **57,** 1344–1371 (2013)
17. https://goo.gl/j4CzZp
18. https://goo.gl/TZucR6
19. https://goo.gl/pj3vrk

20. NIST 2 The Smart Grid Interoperability Panel—Cyber Security Working Group, Guidelines for smart grid cyber security, NISTIR 7628, 1–597 (2010)
21. Z. Lukszo, G. Deconinck, M.P.C. Weijnen, *Securing Electricity Supply in the Cyber Age—-Exploring the Risks of Information and Communication Technology in Tomorrow's Electricity Infrastructure* (Springer, 2010)
22. I.L.G. Pearson, Smart grid cyber security for Europe. Energy Policy **39**, 5211–5218 (2011)
23. P. Anghelescu, E. Sofron, S. Ionita, L. Ionescu FPGA implementations of cellular automata for pseudo-random number generation, in *The 29th International Semiconductor Conference*, CAS 2006, Sinaia, Romania, 27–29 Sept 2006, IEEE Catalog Number: 06TH8867, ISBN 1-4244-0109-7, pp. 371–374, WOS: 000243090700078 (2006)
24. P. Anghelescu, S. Ionita, G. Iana, High-speed PCA encryption algorithm using reconfigurable computing. J. Cybern. and Syst. **44**(4), 285–304 (2013) (Taylor & Francis), https://doi.org/10.1080/01969722.2013.783375. ISSN: 0196-9722, WOS: 000320016100001
25. P. Anghelescu, FPGA implementation of programmable cellular automata encryption algorithm for network communications. Int. J. Comput. Syst. Sci. Eng. (CSSE) **31**(5). ISSN: 0267-6192, WOS: 000393361100003, Sept 2016
26. F. Bîrleanu, N. Bizon, "Reconfigurable computing in hardware security—a brief review and application. J. Electr. Eng. Electron. Control Comput. Sci (JEEECCS) **2**(1) (2016)
27. E.D. Knapp, *Industrial Network Security—Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems* (Syngress, 2011)
28. C. W. Probst, J. Hunker, D. Gollman and M. Bishop," Insider Threats in Cyber Security", Springer, 2010
29. M. Chowdhury, A. Apon, K. Dey, *Data Analytics for Intelligent Transportation Systems* (Elsevier, UK, 2017)
30. J. Graham, R. Howard, R. Olson, *Cyber Security Essentials* (CRC Press, 2011)
31. A. Ashok, A. Hahn, M. Govindarasu, Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment. J. Adv. Res. 5:481 (2014)
32. B. Genge, I. Kiss, P. Haller, A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. Int. J. Crit. Infrastruct. Prot. **10**, 3–17 (2015)
33. C. Tu, X. He, Z. Shuai, F. Jiang," Big data issues in smart grid—a review. Renew. Sustain. Energy Rev. **79**, 1099–1107 (2017)
34. N. Nezamoddini, S. Mousavian, M. Erol-Kantarci, A risk optimization model for enhanced power grid resilience against physical attacks. Electr. Power Syst. Res. **143**, 329–338 (2017)
35. H.R. Nemati, L. Yang, *Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering* (Information Science Reference, 2011)
36. Pricop E. Research regarding security of control systems. Ph.D. Thesis, Romanian Title: Cercetari privind securitatea sistemelor automate, Petroleum-Gas University of Ploiesti, Ploiesti, Romania, 2017
37. MITRE Corp.—CVE Database Website, https://goo.gl/zh6qTC
38. Nexpose (Rapid 7) Website, https://goo.gl/kgTjLW
39. OpenVAS Website, https://goo.gl/nGSYnd
40. Nmap Website, https://goo.gl/MU9mpA
41. Nessus Website, https://goo.gl/VrpDBr
42. E. Pricop, S.F. Mihalache, J. Fattahi, Innovative fuzzy approach on analyzing industrial control systems security, in *Recent Advances in Systems Safety and Security* (Springer International Publishing AG, Cham, Switzerland, 2016) ISBN: 978-3-319-32523-1
43. E. Pricop, S.F. Mihalache, Fuzzy approach on modelling cyber attacks patterns on data transfer in industrial control systems, in *3rd International Workshop on Systems Safety and Security—I-WSSS 2015—Proceedings of the 7th International Conference on Electronics, Computers and Artificial Intelligence*—ECAI 2015, vol. 7, SSS-23–SSS-28, nr. 2/2015 – ISSN: 1843-2115. ISBN: 978-1-4673-6646-5
44. E. Pricop, S.F. Mihalache, Assessing the security risks of a wireless sensor network from a gas compressor station, in *2nd International Workshop on Systems Safety and Security—IWSSS 2014, București, România—Proceedings of the 6th International Conference on Electronics,*

Computers and Artificial Intelligence—ECAI 2014, vol. 5, pp. 45–50. ISBN: 978-1-4799-5478-0
45. E. Pricop, S.F. Mihalache, N. Paraschiv, J. Fattahi, F. Zamfir, Considerations regarding security issues impact on systems availability, in *4th International Workshop on Systems Safety and Security—Proceedings of the 7th International Conference on Electronics, Computers and Artificial Intelligence*—ECAI 2016, vol. 8, No. 4/2016, ISSN: 1843-2115, Ploiești, România (2016)
46. M.H. Lopez, Resendez C.F. Lerma, Honeypots: basic concepts, classification and educational use as resources in information security education and courses, in *Proceedings of the Informing Science and IT Education Conference InSITE* (2008)
47. P. Sokol, J. Host, Evolution of legal of honeynets, in *Recent Advances in Systems Safety and Security* (Springer International Publishing AG, Cham, Switzerland, 2016) ISBN: 978-3-319-32523-1
48. Conpot Honeypot Website, https://goo.gl/sZfER8
49. Honeynet Project Website, https://goo.gl/rw9kCx
50. Dionaea Honeypot Website, https://goo.gl/wNvq98
51. Cowrie Honeypot Website, https://goo.gl/N8dVE7