CYBER SECURITY OF SMART GRID AND SCADA SYSTEMS, THREATS AND RISKS

Hossein Hooshmandi Safa
MEEDC – Iran
hosein.hoshmand@gmail.com

Davood Mohammadi Souran
MEEDC – Iran
davood_souran@yahoo.com

Mehran Ghasempour
MEEDC - Iran
ghasempour.mehran@gmail.com

Amir Khazaee
MEEDC – Iran
amir.khazaee@ymail.com

ABSTRACT

Nowadays electricity is one of the most significant requirements and base of life facilities. Any interruption in supplying and providing power, like widespread blackouts will cause irreparable effects on different aspects of a society. Technology increasing progress provides remote control and monitoring of power grid through the supervisory control and data acquisition (SCADA) system and substation automation which decreases the costs of power transition and control, increases the efficiency and motivates to smart grid. These kinds of technologies create new opportunities to remote monitoring and control of the power substations and equipment for the regional electricity companies. Some of these achievements have been used before but modern systems provide more facilities in operation and maintenance of power system. It is noticeable that this opportunity may convert to threat if cyber security encounters with lack of attention in the smart grid. Therefore, providing sensitive and secure equipment is one of most significant and vital problems to increase the cyber safety and decrease cyber-attack risk in the smart grid.
Therefore the facilities equipment, their risks and vulnerabilities should be detected and appropriate methods should be propounded to encounter with these problems. In this paper, substructures of smart grids are firstly discussed. After this introduction, threats, risks and security requirements will be considered in the smart grid. In the following, different types of cyber-attacks and the best architectural and security strategies will be offered.

INTRODUCTION

The TCP/IP protocol suit is widely used in the local and wide area smart networks for advanced digital substation automation. It can be used in different operating systems such as Windows and UNIX. These technologies create new opportunities, such as remote access for supervisory. Some of these applications have existed previously. But modern system provides a wide range of operations and maintenance services (such as monitoring control and parameter settings [1]).
Substation automation is done by a special multi-protocol infrastructure in Iran. On the other hand, if the law and the security situation have not been respected, usage of these protocols creates different risks to the electricity network and may change an opportunity to a threat. For example, non-compliance with security measures might cause blackouts in the country. To prevent these risks, it is necessary to identify the threats and risks associated with the smart grid in the beginning. The following sections introduce the smart grid infrastructure needs and requirements of relevant security.

INTRODUCE THE SMART GRID

Smart grid has different interpretations, including modernization, development of rapid response and optimal management of power networks by using communication systems and technology. Intelligent systems consist of generation, transmission, distribution, subscribers, operators, service provider and the electricity market. These parts are connected together as shown in Figure 1.

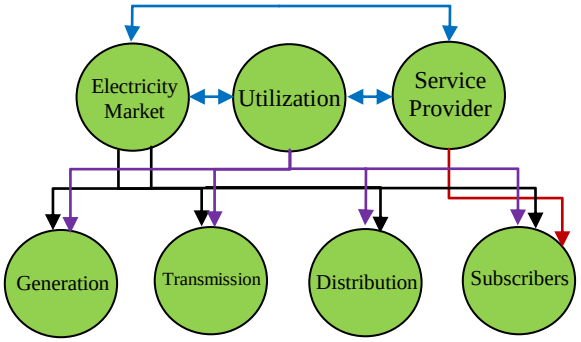

Figure 1: Connection between different parts of smart grid

Service provider: It is responsible of the task of storage, maintenance, Distributed Generation (DG), billing and account management. It is able to publish the billing of all infrastructures like water and gas.
Common sections: It includes business, industrial, agricultural, domestic and measured by device (smart meters) and other related areas. In the subscribers section, it provides power consumption management, distributed generation, resource optimization and cost management.
Electricity market: The electricity market creates the optimum mode for the better management of generation and consumption equality in the electricity market.
Generation: this section is the responsible of renewable energy generation, such as wind power, solar, geothermal and nonrenewable such as combined cycle power plants.
Distribution: It is responsible of the electricity transition to the consumption areas.
Utilization: It is responsible for functional operation of the network by energy management systems, distribution management systems and training the personnel.
Transmission: High-voltage produced by power plants is transformed to the distribution is done by this section. This field includes distribution and transmission lines and substations.

Because of the great advantages of smart grid such as high performance, high reliability, low operational costs, etc., in the near future, the current power grid will be replaced by these systems. The move to mechanization process in the power network by using IT infrastructure will be a turning point in these networks.

SECURITY GOALS

There are three approaches when looking for a definition of security for some of the systems. The first view is that how an attacker may access to the system information. This question provides network security counter measures. The second view is identification of the principles of security against threats, or in other word show to achieve security goals. Seven security purposes can be used in the different systems as follows:

1) Confidentiality: This goal is defined as the purpose for preventing the disclosure of information by unauthorized individuals or systems.
2) Safe Information: This goal means to avoid changing information by unauthorized individuals or systems undetectably. This includes defense against attacks on information obtained through the injection of messages, broadcast messages, and message latency in the network. Violation of the safe information may cause damage to the equipment or people
3) Accessibility of information: It is necessary to ensure no unauthorized access to information or systems or unauthorized use of authorized users.
4) Authentication: It is defined to identify the actual identity of the user and mapping this identity to an internal management systems and publishing a license. The other goal of a license is the establishment the distinction between legitimate and illegitimate users based on identity.
5) License: Detecting between legitimate and illegitimate users is a necessary task to access control and prevent the unauthorized individuals or systems to access to the system
6) Audit and inspection ability: With the aim of inspection and using administrative records, the system behavior can be determined.
7) Protection of third parties: to prevent damage by third parties through the system of information technology. DDoS1 attacks or worm attacks are examples of this type of injuries.

The third point of view for a special system with regard to safety standards is a special system for achieving the objectives of relevant security goals. Safety standards mean the formal certificates or standard levels defined official security and methods. Typically attacks and new vulnerabilities reduce the security level in the safety mechanisms of the system with time. It is necessary to update the security architecture on a regular basis and in emergencies [2].

DIFFERENT TYPES OF ATTACKS

In any industrial network, depending on the specific functions and safety objectives of the environment different subsets of security goals are defined. The attack is the deliberate violation of these security goals. The attack scan be performed by people inside or outside the organization. Attacks are classified into two categories, directed and in discriminate. In discriminate attacks imposes further damage to the system if the system is very vulnerable.

But targeted attacks, (for specific purposes), such as industrial espionage, war or terrorism, are meditated to harm a particular communication system and contains a gathering information step before the attack. Some of these attacks are:

DOS2 Attack: the attacker reduces the system performance against targets.

Espionage: will track information to violate the confidentiality of communications LAN or wireless communication network.

The system gap: The attacker can close the gap through authentication and access control, and behavior of the system, including confidentiality and accuracy of the information requests related to the control center which usually involves consecutive influence on various systems and promotion as a step forward.

The virus is based on the creation of malicious code by an attacker to bypass authentication mechanisms, access control and unwanted data injection. This kind of codes is injected by the legitimate users to the system.

Viruses often directly or indirectly decreases the ability of infected systems due to the high processing requirements and bandwidth.

Worms are malicious code that their mechanism depends on automatic identification and exploitation of system vulnerabilities without user intervention. Worms spread indiscriminately and often make difficulty to access to the system. Besides of this, it is possible that worms have been designed to start a targeted attack to infect computers around [2].

THREATS TO THE SECURITY OF THE REMOTE CONTROL NETWORKS

Network attacks are divided into two categories:

Non- effective attacks

Espionage attack is non effective, which has no direct damage. However espionage ends to find useful information that can be used for an active attack.

Active attacks

In most cases, the network attacks provide physical access to parts of the network. Forging is an active attack in which an attacker without permission can edit, add or delete data on the network. The control commands may

have changed by the attacker. The RTU can be activated or deactivated by a false alarm. Another active attack from the forging type is the broadcasted and repeated traffic. Espionage and forgery can be prevented by encryption [3].

SNMPv3 security:
In the security model, SNMPv3 is developed to the user authentication; data validation and protection against disclosure repeatedly send the message. Administrators can create specific permissions for each user to have SNMP access. This has a great impact on security. There is no need to reconfigure the SNMP requirements to remove user access to facilitate scanning system.

Other proposals to enhance the security:
To protect the network and the interface layer, IPsec and TLS protocols such as network security services have been proposed. If the remote control system is based on the TCP/IP, it is needed to implement IPSec or TLS.

Problems in the use of open protocols:
Because the network frame in an industry is an attractive attack goal, the use of free software Net-SNMP, NTP and SSH is not recommended. It is necessary to utilize appropriate network protocols to keep the remote control of network security. Furthermore, when designing a security system or protocol, security should be considered.

SCADA NETWORK, METHODS AND SECURITY TECHNOLOGIES

Network sections, routing and management of information transition should have sufficient security while it may have different layers. Security levels are selected based on risk assessment and administrative requirements [4], [5].

Topology, routing and protocols

Ensure the reliability of the network topology by using the plug-in which provides network topology that contains layers with RSTP in the LAN post, OSPF on the intranet and VRRP to access to the IP network and supporting links between routers. In addition, it is possible to increase security by separating VLAN traffic. The LAN, OSPF on the intranet and VRRP for access to the IP network and back up links between routers is doubly. It is possible to separate VLAN from traffic to increase security. Some protocols, such as IPv6, OSPFv3 (RFC 2740) and SNMPv3 (RFC 3826) are independent authentication mechanism and data encryption. Routers and switches should send messages with mechanics such as PQ, CBWFQ or mechanisms to be prioritized queue [4].

Authentication of users and requirements

Most cases of AAA and equipment are used for user authentication. When the password is sent over the network it must be encrypted. It is essential for the use of some types of cryptographic such as hash functions that are approved for FIPS and prevent repeated attack scan be sent. It also proposed to use the password or complementary password such as fingerprints in the physical environment. Role-based access control is based on tasks assigned to users. All communication systems managers must be recognized, confidential and managed as a single unit [4].

SSL/TLS method

SCADA systems security increases with using SSL/TLS protocols. In the last decade, secure communication channel SSL/TLS has been a virtual private network for Internet users and it is used for secure communications over TCP/IP. Secure communications SSL/TLS certificate is done by confirming the interaction between client and server using and creating digital signatures and encryption. These protocols are very practical ways to fight with a man in the middle attacks and send data back which are managed and controlled by the IETF. These protocols have fundamental limitations like high executive pay, lack of services and reliable transport protocols such as TCP and non-repudiation [5].
The channel protocol insurance creates only digital signatures and encryption communications, which making them more powerful and non- resistant against attacks based on traffic analysis.

IPsec VPN

General IPsec VPN for fire walls are placed between the router and landscapes whenever is necessary. IPsec provides assurance for the integrity, accuracy and reliability of the data provided. In this method, each IP packet is protected in a compartment encrypted packets which are allowed to enter the bus range.
Routers use the new IP to send packets of data messages between the end points use their bus. At the end, the packets are modified. The IPSec protocol is placed below the SSL/TLS (Figure 2), but many of the its related security services security are similar to SSL /TLS security protocols [4], [5].

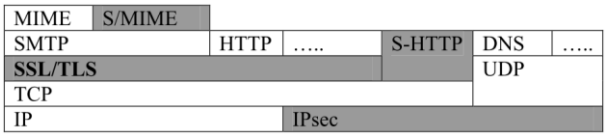

Figure 2: Security Protocol Stack [4]

CONCLUSION

Design and development of smart grid should consider cyber vulnerabilities in the old grid. The known vulnerabilities in the current electricity grids must address and comply with the implementation of smart grid technology. The development of smart grid increases the complexity of the system. Therefore new communication routes are added to the system. The increasing complexity and communication routes are developed to increase the

damage driven by the cyber-attacks. The prediction of how the attacks may be exposed will become difficult when the size of the smart grid implementations (millions of units) increased and unpredictable savvy competitors are trying to develop new kinds of attack. Moreover, the goal is to resist the attacks against the desirable properties of the smart grid such as the optimization of resources and efficient performance in the competition features.

Minimizing costs and providing a higher priority are counted in comparison to security in the face of a threat that is not yet known. There must be a concerted effort and security of smart grids in progress to include the full life cycle development.

This development includes the requirements, design, implementation, testing, evaluation, acquisition, installation, commissioning and maintenance. A failure in any phase of the life cycle reveals defects that lead to system vulnerabilities and can be exploited by a skilled attacker Each of the smart grid components has lifecycle security. It is necessary to have a predefined development period with emphasis on safety, including independent accreditation authority to ensure the prevention or struggling with the attacks. It should be noted that the requirements, design, implementation and operation of multi-level defenses are necessary to prevent the tragic consequences of new lesions or new attackers to reverse some of the defense mechanisms of the system forms.

REFERENCES

[1] F. Lenoir, A. Vidrascu, J.M. Delbarre, 2006, “Cyber Security in Substation Automation: Design and Supervision”, *Cigré 2006 Paris Session*.

[2] Dacfey Dzung, Martin Naedele, Thomas P. von Hoff, Mario Crevatin, 2005, "Security for Industrial Communication System", Proceedings of the IEEE, Vol.93, NO. 6, June 2005

[3] Gemma Sánchez, Isabel Gómez, Joaquín Luque, Jaime Benjumea and Octavio Rivera, 2010 "Using Internet Protocols to Implement IEC60870-5 Telecontrol Functions", *IEEE Transactions on Power Delivery*, (Volume:25, Issue:1)

[4] Farkhod Alsiherov, Taihoon Kim, 2010, “Research Trend on Secure SCADA Network Technology and Methods” *WSEAS Transactions on Systems and Control*, Volume 5 Issue 8, Pages 635-645

[5] James H. Graham, Sandip C. Patel, 2004, “Security Considerations in SCADA Communication Protocols”, *Intelligent Systems Research Laboratory, Technical Report TR-ISRL-04-01*, September 2004