International Journal of Advances in Computer Science & Its Applications – IJCSIA 2018
Copyright © Institute of Research Engineers and Doctors , SEEK Digital Library
Volume 8 : Issue 2- [ISSN : 2250-3765] - Publication Date: 28 December, 2018

Assessment of Global Cyber Security Challenges with special focus on Electricity Sector of Malaysia

S M Salim Reza

Abstract- **Recurrent events of cybercrimes happening around the globe recently which are affecting individual from different levels, cybersecurity has become has become an essential part of any academic and professional discussion related to modern communication technologies involving commercial and governmental entities. The key objective of this study is to find out the weakness and loopholes related to cybersecurity which is particularly related to the electricity sector of Malaysia. It has been identified that rolling out of the smart grid system may have many benefits in the long run. However, this may also unlock new potential threats from cyber attackers as the security of the smart meters are not highly developed yet and those are connected to the server and global network through channels with low level of security. This paper discusses the possible implications if a smart metering system is compromised and how to prevent such events, such as, by producing replicas of SCADA system to operate uninterruptedly without any major damages even in case of an unavoidable security breach.**

Keywords- **Cybersecurity, Smart Grid, Network Security, Cybercrimes in Electricity Sector**

I. Introduction

Safeguarding an organization or entity from physical threats and attackers is not adequate any longer, rather, in several scenarios it is even more important to maintain the cybersecurity and protect it from cyber attackers by identifying and promptly addressing the weaknesses [1], and it is even more prominent factor to consider while dealing with electricity sector as it involves significant public interest.

The electricity production and distribution sectors have now become increasingly digitalized and decentralized and with advent of modern technologies and globally connected networks, the number of cyberattacks has also increased in recent years compared to previous decades [2].

In the conference of World Energy Congress, cyber security vulnerabilities and threats were identified as the key source of threats for energy and utility sectors worldwide by the speakers and the amount of threat of even more prominent of organizations and systems that are highly digitalized such as a smart metering system [3]. This paper highlighted the forthcoming technological changes that are happening in the electricity sector of Malaysia toward an automated and modernized system as smart grid system is being rolled out and how these could make it susceptible to the new pattern of cybercrimes. Existing security measures are also analyzed in this paper to identify valuable recommendations particularly for the Malaysian government so that they could apply those measures to safeguard against potential cyber security threats.

II. Power Generation & Distribution Sector of Malaysia: Current Scenario & Potential Threats

A. *Overview*

Smart meter, an integral component of smart grid is no different than a typical IoT device which is connected to a wide area network and is used for maintaining real time communication and monitoring. Hence, electricity production and distribution no more operate as a closed system, and the connectivity of a smart grid has made it vulnerable to the institutional and coordinated cybercrimes. Such an event occurred for the first time in December 2015, when a team of organized cyber criminals were able to hack the network of Ukrainian power grid and seized control [4]. Three substations were affected due to the intrusion, and the number of affected customers totaled 225,000. Surprisingly, the grid controllers found themselves without any electricity as the hackers also demobilized the UPS

S M Salim Reza
University Kebangsaan Malaysia

system that was used for supplying emergency power backup to the system. The threat of such a cyber threat is so prominent nowadays that according to a recent survey conducted among prominent power sector professionals globally, 72 percent has termed the importance of cyber security for a utility company as “important” or “very important” for uninterrupted grid operation [5].

There are three key levels of security threats for a smart grid from which it is necessary to be protected [6]. Primarily, the instruments itself including power appliances and the smart meters are physically accessible to external attackers, and it is possible to interfere the signal that they broadcast to the concentrator nodes. On the next level, the web-based applications can be hacked externally to manipulate the signals that travels through the concentrator nodes to the control centers at remote places. On the tertiary level, the user data that are collected through different value-added applications and user interface, are not immune from attackers.

Supervisory control and data acquisition (SCADA) systems are among the most important elements of a smart grid, which if compromised can bring the entire system down for a significant time. This is basically a computerized system to continuously and automatically control the overall activities of an equipment through data that are collected and examined in real time by using many sensors [7]. In the year 2010, a nuclear powerplant in Iran was under coordinated cyber-attack as the attackers seized control of the SCADA network with a malware called Struxnet [8]. According to CTO of cybersecurity consultancy firm AlgoSec, Dr. Avishai, in general the SCADA systems are not usually very efficient to identify differences between a genuine request received from sensors and a false signal received from a malware [9].

B. Malaysia’s transition toward Smart Grid and potential threats

Energy Commission of Malaysia, the policy development & authoritative body for the country’s electricity generation and distribution, is now upgrading the capacity of its national grid, which is consists of 420 major substations connected through over 11,000 kilometers of transmission and distribution lines throughout the peninsula [10]. Malaysia also aims to achieve connectivity with ASEAN Power Grid (APG) by the end of 2019 [11]. The initial step toward transition toward smart grid system from a traditional set up begins with the installation of smart metering system for the end users. Similar to typical IoT devices smart meters support real-time communication with the network and automatic firmware upgradation, as it transmits energy usage data to the system using Transmission Control Protocol/ Internet Protocol (TCP/IP) [12]. The data center of a smart grid analyzes the real-time data received from the meters and controls production accordingly with real-time communication with power generation units. 1000 smart meters were installed across Putrajaya and Melaka through Tenaga Nasional Berhad’s (TNB) with government funding in 2013 and the goal of the pilot project was to gather practical experiences for all parties involved including identifying the security vulnerabilities and how to avoid them.

Many cybersecurity experts believe that due to continuous connectivity with external network, it is possible for attackers to hack a smart meter from outside [13], and it is possible to disrupt power supply to the individual or collective unit connected with the smart meter, which could also be done by terrorists with an ill intension. Cybersecurity researcher Netanel Rubin from security firm Vaultra believes that a single line of corrupted code could hack the smart meters which are used in UK at present [14]. On top of disrupting power supply to the user, a compromised smart meter may also cause massive overflow of electricity to the system leading to explosion and damage to other electrical appliances. Another issue of concern is that since in most of the cases, smart meters used in a locality come from a single manufacturer, their security protocols are also similar. Hence, every connected smart meters under a local network may be exposed to attacks if one of these fail under attack.

III. Recommendations to prevent Cyber-attacks

A. Existing global practices

Each of the globally followed safety measures to prevent cybercrimes has their advantages and disadvantages which needs to be evaluated in comparison to analyze their individual effectiveness.

- *Multi-factor Authentication (MFA):*

MFA allows the system to verify a user using two or more levels of security checkpoint or “claims”, presented by the user [15]. The procedure is frequently referred as 2-step verification, 2-factor authentication (2FA), step-up verification, advanced authentication and so on in the industry. MFA is appreciated due to its ability to compensate the vulnerabilities of each element with strength of others. Such as by adding a level of authentication code delivered to a mobile device such as mobile phone or code generator it is possible to protect the knowledge elements including passwords, secret number, security questions from brute force attack or organized social engineering [16]. In 2016, the global market for MFA stood at a value of USD 5.22 billion, which is estimated to be worth of USD 12.5 billion in 2022 [17]. As the technologies associated with MFA is being developed over time, a large number of provincial and federal compliance standards across different countries now require organizations to integrate MFA as a primary level of authentication method [16].

Despite having a set of very strong advantages, wide scale implementation of MFA is also hindered by a number of setbacks. The first factor of concern is increased cost of implementation. Added cost would be incurred from a number of sources including mobile application platform design, payment to SMS gateway services, integration of Application Programming Interface (API) with the system, maintenance of the hardware and software-based tokens and other administrative costs including training of staff members [18]. Another matter of concern is to have a backup method of authentication in case of token generating hardware or cellphone is lost and the user is not able to receive an OTP [19]. Moreover, SMS OTP, which is the most widely used MFA service worldwide, has been discovered to be the weakest among all to cybercrimes [20]. For example, a trained hacker may easily be able to hack the SS7 network used by SMS OTP to create a diversion so that the OTP goes to his mobile device instead of the user's. Due to this reason, U.S. Department of Commerce's National Institute of Standards & Technology (NIST) has officially advised the technology companies not to use SMS OTP as a verification method [21]. Finally, another challenge of MFA is to ensure the user's convenience. For instance, carrying a separate hardware token for authentication is usually not convenient from a user's point of view. To overcome it, software based token can be used which consists automated code generation technic [22].

- *Sandbox*

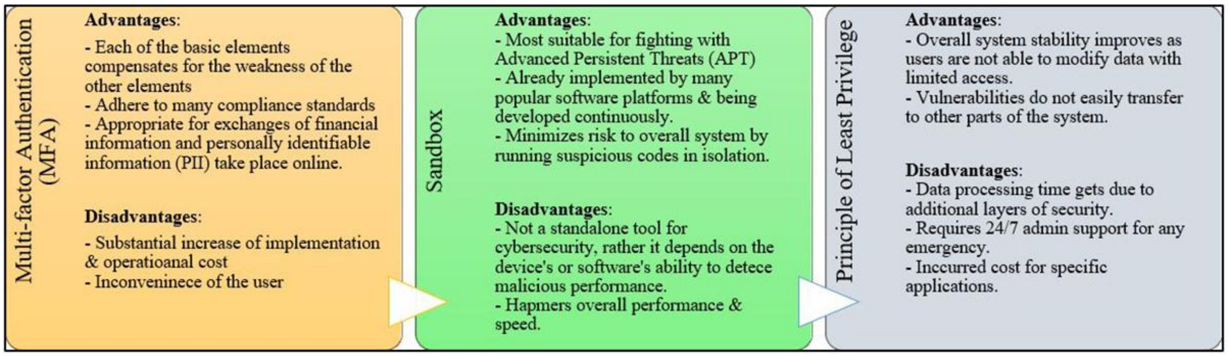
Sandbox is a process of running potentially malicious, unauthenticated applications in a separate and isolated setting where their behavior could easily be analyzed without making any damage the other programs or the core operating system itself [23]. Sandbox can enhance the security of a smart grid from multiple types of attack including Advanced Persistent Threats (APT). Within a typical data lake architecture, sandbox acts as an isolated closed environment to analyze and process data received from different sources without putting any impact on the integrity of the system [24]. Hence a sandbox often helps developers to examine a prototype before large scale deployment in any applicable systems and it helps to maintain data security of the system.

Sandbox has been gaining popularity globally in the recent years as the technology is becoming advanced with new features. Several online gateways, threat mitigation vendors, firewall and web applications has included sandbox within their system [25]. Adobe's Acrobat and Flash environment are among the early software to incorporate sandbox, which was mainly used for preventing unintended system crash due to malicious codes [26]. Sandbox was also a part of Google Chrome's one of the early releases during 2008 [27].

The key challenge of utilizing sandbox to protect data integrity begins with the fact that its effectiveness eventually depends on the design, strength and architecture of the device or software where it is used, because it is the responsibility of the software or device to identify potential threats & malicious agents and send to sandbox for examining their behavior. It is not wise to consider sandbox as an independent data protection tool, rather to protect the system it requires coordinated and collaborative effort of all involved tools including security protocols, software, policies and products. The issue was extensively stipulated in the official release notes of both Google Chrome and Adobe. It was stated that the operating system's overall defense from the malware would determine the ultimate success and stability of the sandbox environment [28]. Moreover, the FAT32 which is a traditional file system being used by many USB devices, computers and storage devices does not support sandbox as it does not have additional layers of security descriptors [27]. Besides, sandbox method may also slow down the overall system specially the older ones due to processing data through an additional security level. According to cybersecurity research scientist Chris Valasek, implementation of sandbox requires a balance between security and functionality. It is, therefore, essential for organizations to find out properly about how much work efficiency and speed they could forego by implementing sandbox and whether the additional security level is worth it [29]. Particularly for computational operations involving a massive amount data may slow down significantly even with the slightest changes in processing of single computation. The complexity could also make the user experience difficult and complicated.

- *Principle of Least Privilege (PoLP)- granting the user minimal access to the system*

PoLP is a process of limiting access for users and computing system only to specific resources of a system which they must require to complete their desired operations depending on their level of hierarchy, through proper authentication and predefined schedule of operation [30]. If a larger network such as smart grid wants to allow limited access to user of individual smart metering units, other network connected units, PoLP can easily control their access level based on how much accessibility and resources they will actually need. This aids the large network to protect itself from falling victim to cyberattacks. A recently study done by Forrester Research has identified unverified and uncontrolled access to the network as one of the major causes behind large scale cybercrimes [31].


Multi-factor Authentication (MFA)

Advantages:
- Each of the basic elements compensates for the weakness of the other elements
- Adhere to many compliance standards
- Appropriate for exchanges of financial information and personally identifiable information (PII) take place online.

Disadvantages:
- Substantial increase of implementation & operatioanal cost
- Inconveninece of the user

Sandbox

Advantages:
- Most suitable for fighting with Advanced Persistent Threats (APT)
- Already implemented by many popular software platforms & being developed continuously.
- Minimizes risk to overall system by running suspicious codes in isolation.

Disadvantages:
- Not a standalone tool for cybersecurity, rather it depends on the device's or software's ability to detece malicious performance.
- Hapmers overall performance & speed.

Principle of Least Privilege

Advantages:
- Overall system stability improves as users are not able to modify data with limited access.
- Vulnerabilities do not easily transfer to other parts of the system.

Disadvantages:
- Data processing time gets due to additional layers of security.
- Requires 24/7 admin support for any emergency.
- Inccurred cost for specific applications.

Figure 1: Comparative Analysis of Advantages and Disadvantages amongst MFA, Sandbox, and PoLP

A smart grid consists of a number of individual elements and IoT devices such as control and data center, admin panels, generation and distribution units, and smart meters, and each element has their own vulnerabilities [32]. Hence, instead of having a particular technology to protect the entire smart grid from cyberattacks, it is more recommended to have a combination of preventive measures. Apart from implementing the sophisticated and advanced security measures such as MFA, Sandbox and PoLP, a smart grid should also include some basic or fundamental security and data protection features, which are illustrated in the following-

- Smart meters and the service providers should always keep a record of each data and log it into a secured server. Such data should include but not limited to exact electricity usage, password modifications, billing history, payment records and so on [33]. For example, Indian government's official electricity guidelines require all smart metering authorities to maintain accurate data records into their system, and give access to the data through PoLP standard so that users cannot make any modification to the data [34].
- Authenticity, accuracy and integrity of collected data should be analyzed and examined through both automatic and manual methods, and any discrepancies should be reported and addressed properly and early to prevent further damage [35].
- Adequate training should be provided to all concerned officials and technical persons. There should also be specific guidelines on individual's roles in case of an unavoidable security breach [36].
-
- Customization of a SCADA system should only be done by a highly skilled team of professionals considering the complexity of the operations.
- Security for Smart Electricity Grid (SEGRID), a project funded by European Union [37] recommended a security measure by replicating the operation of SCADA system, and allows the replicas to operate uninterruptedly and without any error even if a cyberattack cripples the main system.

IV. Conclusion

Internet connectivity of a large number of home and official appliances and advancement of IoT devices, have made cybersecurity more significant than ever. To maximize the benefit, it is now crucial to always stay aware of security loopholes within a system and possess solid knowledge on how to overcome them. It is also essential to note that damage done by a coordinated and advanced level of cybercrime could be way more upsetting for an organization or household than a traditional robbery could make. The recommendations in this report are mainly derived based on the key progresses and proceedings happened in the information security industry and electricity sector within last couple of years. Further investigation and research to derive more recommendations can be conducted, which would be even more viable for users and companies to arrange in both short term and long term.

V. References

[1] Veritech Systems, "Why Cyber Security is Important for the Modern Business," 11 Julu 2017. [Online].

[2] D. Healey, S. Mechlar, U. Antia and E. Cottle, "Cyber Security Strategy for the Energy Sector," European Parliament, Brussels, 2017.

[3] Swiss Re Corporate Solutions and Marsh & McLennan Companies, "The road to resilience: managing cyber risks," World Energy Council, Berlin, 2016.

[4] H. K. Trabish, "Why utilities say grid security is the most pressing sector issue of 2017," 10 April 2017. [Online].

[5] UtilityDive, "The State of Electric Utility 2017," UtilityDive, 2017.

[6] F. Skopik, Z. Ma, T. Bleier and H. Grüneis, "A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures," *International Journal of Smart Grid and Clean Energy*, vol. 1, no. 1, pp. 22-28, 2012.

[7] H. Kim, "Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks," *International Journal of Distributed Sensor Networks* , 2012.

[8] T. Bradley, "Stuxnet Compromise at Iranian Nuclear Plant May Be By Design," PCWorld, 2010.

[9] T. Bradley, "SCADA Systems: Achilles Heel of Critical Infrastructure," PCWorld, 2011.

[10] Energy Commission of Malaysia, "The National Grid-Strengthening Malaysia's Framework," Energy Commission of Malaysia, Kuala Lumpur, 2017.

[11] T. Ahmed, S. Mekhilef, R. Shah, N. Mithulananthan, B. Horand and M. Seyedmahmoudiand, "ASEAN power grid: A secure transmission infrastructure for clean and sustainable energy for South-East Asia," *Renewable and Sustainable Energy Reviews*, vol. 67, pp. 1420-1435, 2017.

[12] Smart Energy Great Britain, "Smart meters explained," Smart Energy Great Britain. [Online].

[13] S. Meadows, "Six reasons to say no to a smart meter," The Telegraph, 2 August 2017. [Online].

[14] A. Hern, "Smart electricity meters can be dangerously insecure, warns expert," The Guardian, 29 December 2016. [Online].

[15] P. Ihalainen, "What is Multi-Factor Authentication (MFA)?," Globalsign, 2016.

[16] M. Dacanay, "Benefits of Implementing Multiple Factor Authentication," Globalsign, 2017.

[17] Markets and Markets, "Multifactor Authentication Market by Model (Two-, Three-, Four-, and Five-Factor), Application (Banking and Finance, Government, Military and Defense, Commercial Security, Consumer Electronics, Healthcare), and Geography - Global Forecast to 2022," 2017.

[18] S. Carter, "The Challenges and Benefits of Multi factor Authentication - MFA 101, Part 2," 2017.

[19] Microsoft Azure, "Getting started with the Azure Multi-Factor Authentication Server," 2016. [Online].

[20] inWebo, "Why is MFA security even a question?," inWebo, 2017. [Online].

[21] P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr and J. P. Richer, "Digital Identity Guidelines: Authentication and Lifecycle Management," National Institute of Standards and Technology.

[22] inWebo, "The 5 Most Common Challenges of MFA – A Simple Guide to Analyzing Solutions," inWebo, 5 December 2017. [Online].

[23] F. Dickson, "Network Security Sandbox Market Analysis: APTs Create a “Must Have” Security Technology," Frost & Sullivan, 2015.

[24] D. Meyers, "Advantages of the Analytics Sandbox for Data Lakes," BlueGranite, 2016.

[25] N. Lewis, "How sandboxes benefit network protection and malware defense," TechTarget.

[26] T. Bradley, "Why a "Sandbox" Makes Adobe Reader More Secure," PC World, 2010.

[27] N. Sylvain, "A new approach to browser security: the Google Chrome Sandbox," Google Chrome, 2008.

[28] C. Hoffman, "Sandboxes Explained: How They’re Already Protecting You and How to Sandbox Any Program," How to Geek, 2013.

[29] Dark Reading, "The Pros And Cons Of Application Sandboxing," InformationWeek IT Network, 2012.

[30] M. Miller, "What Is Least Privilege & Why Do You Need It?," BeyondTrust, 2016.

[31] M. Sendze, "Managing least privileges from the Cloud," GSN: Government Security News, 2012.

[32] Office of Electricity Delivery and Energy Reliability, "Grid Modernization and the Smart Grid".

[33] C. Curtland, "Energy Management 101: Smart Submetering and Data Logging," Buildings Education, 2014.

[34] Central Electricity Authority, "Functional Requirement of Advanced Meteting Infrastructure (AMI) in India," 2016.

[35] S. Marcello, "Ensuring data integrity: Is manual entry or automated extraction more reliable?," OPIN, 2016.

[36] T. Yardley, S. Uludag, K. Nahrstedt and P. Sauer, "Developing a Smart Grid cybersecurity education platform and a preliminary assessment of its first application," in *Frontiers in Education Conference (FIE)*, Madrid, 2015.

[37] Security for smart Electricity GRIDs, "How to address the security challenges in Smart Grids," SEGRID, 2017.

About Author:

S M Salim Reza is a PhD researcher on Cyber Security, at the National University of Malaysia (Universiti Kebangsaan Malaysia). He is successfully doing his PhD research; besides, he has many journal publications and conference presentations. His interest is in Cyber Security specially the Security coverage on Server system on Solar Energy and other Electrical Energy system for the National grid of Malaysia. Upon successful completion of these project will help the Electricity Server Security of Malaysian government as well as other countries. Besides, he has been an Assistant Professor (formerly, lecturer) in few universities in Dhaka and Kuala Lumpur for last 14 years.