International Journal of Pure and Applied Mathematics
Volume 118 No. 24 2018
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

Analysis of Cyber Physical Vulnerability Index in a Power Station

*Prabakaran R[1], Asha. S[2],
[1]Research Scholar, SCSE,
VIT University, Chennai.
[2]Assistant Professor, SCSE,
VIT University, Chennai.
Email:praba.karan@vit.ac.in

May 22, 2018

Abstract

Vulnerability assessment is an important criteria for cyber security in the evaluation of threats in a power station. The study of cyber-physical systems for supervisory control and data acquisition (SCADA) systems in a power station is mandatory. This paper provides with the detailed study of different types of vulnerabilities and its impact factor in a power grid. It is very essential to understand the Vulnerability index through network in a power station for further security feature [2]. This framework for vulnerability assessment to evaluate the vulnerabilities in the SCADA systems at three points are access points, scenario points and system points [3]. The vulnerabilities are evaluated using the Common Vulnerability Scoring System (CVSS) on the SCADA systems.

***Key Words*:**Common Vulnerability Scoring System (CVSS)

1 Introduction

Cyber security is a growing field across all facets of business operations. We rely on digital technology to communicate, travel,

work and power our homes, offices and economy. Our daily lives, economic vitality, critical infrastructure and national security depend on a stable, safe and resilient defense against cyber-attacks. The threats being launched every day have driven the need to improve upon the cyber security protective strategies. These improved strategies aim to protect systems and networks around the globe and across personal, business and critical infrastructure boundaries. As power plants work to enhance their cyber security, they are preparing for safe and reliable operation for decades into the future [4].

The power energy industry is in the midst of a renewal. Across the nation, power plants are being licensed for a longer period of time as it is run by the government. The transition of power plants from analog to digital plays an important role in safety and performance. Also it governs several other factors like reliability, capability and longevity of the power plant and there is always a need to integrate robust measures in cyber security.

Some of the attacks on Power sector are Denial of Service (DOS), SQL injection attack, Cross site scripting (XSS), Malware and Phishing [1]. Proven digital protection systems are already in place at power plants around the world to proactively protect against cyber threats to plant safety and control systems.

Once a plant has the appropriate resources, it needs cutting-edge technology to help enhance its cyber protection. The ever-evolving nature of cyber threats means that there is also a need for evolution in the products used to combat those threats. A plant equipped with the most up-to-date cyber threat analysis platform, including unique digital signature tools, endpoint protection and network situation awareness modeling tools, will be better able to detect and mitigate the threat of cyber-attacks.

Cyber Security is always concerned about its major role in infrastructure assets in the power sector through the continuation efforts in the area of security. Through partnerships between the power industry and cyber security providers who possess unique power experience, the industry can be confident that their critical digital assets will be protected. The Nations critical assets and threats are protected by the highly skilled grade A cyber engineers. These power stations have strict regulations that are very difficult to violate. These regulations purely concerns about the safety and

security of the power plants, such that no other industry is best suited for the energy sector in the security aspects. The cutting-edge expertise brought together by the AREVA-Northrop Grumman team is one example of a partnership that takes a proactive, multi-pronged approach to ensure the cyber security of the U.S. power sector, helping utilities meet today's missions and address tomorrow's threats [6].

2 LITERATURE REVIEW

A. Cyber-Physical System Security of a Power Grid: State-of-the-Art

This paper focuses on the deployment of the traditional power grid to smart grids through Information and Communication technologies. In the current threat environment, vulnerability research is incredibly important. These findings can serve to better protect users and make software developers and vendors aware of flaws that could put sensitive information at risk of exposure The increasing vulnerability index has direct impact on the cyber intrusion. During the system upgrades new vulnerabilities may be derived. Therefore it is highly advisable to access the system for vulnerability periodically. As an alternative a test bed that has an impact of cyber-attack analysis is used. A tested should possess the characteristics of the real time system. The design of detection systems should meet the requirements of power systems, such as transmission delay and system performance. An over-designed detection system that bears a high computational burden may reduce the performance of both power system and detection system [5].

B. Cyber-physical Security and DependabilityAnalysis of Digital Control Systems inNuclear Power Plants

In this paper, we discuss about the issues in the cyber physical security and control systems in Nuclear Power Plants. Also a comparison between two cyber security standards namely ISO27001 and RG5.71. ISO27001 is a standard for information security and RG5.71 is a comprehensive approach for cyber security. So, an enhanced cyber framework demonstrates that the proposed framework not only abides by RG5.71 but also prevents the intrusions from outsiders. To reduce the computation complexity, a technique

is employed by partitioning the set of timed transitions into fast- and slow-timed transitions [7].

C. Performance Comparison of Vulnerability Indices on a Practical Power System

This paper is presents a performance comparison on PSL and PLL vulnerability indices, that are used in power grids for accessing various contingencies. The concept behind these vulnerability indices is that PSL index was found to be more accurate than the PLL because it provides with the accurate status of the power system that is considered to be highly vulnerable. These indices could determine the accurate vulnerability index of a system to prevent any attacks or to enhance the emergency control [8].

D. Susceptibility Valuation of Cybersecurity in SCADA Systems

This paper focuses on the key approach in the defense that is used at the present times. Proposed method is based on password model and firewall protection which is considered to be primary mode of protection in power grids. The potential loss of load in a power grid has a total impact on the potential electronic intrusion. The integration of logic based simulation method and a module for power flow consumption is added for its capability. The impact of attacks launched from outside or within the substations is evaluated using IEEE 30 bus system for the improvement of the cyber security [9].

3 OBJECTIVE

The main aim of the proposed paper is to analyze the Common Vulnerability Score of the power plant using three metrics,

- BASE METRICES
- TEMPORAL METRICES
- ENVIRONMENTAL METRICES

4 COMMON VULNERABILITY SCORING SYSTEM

The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. Scores are calculated based on a formula that depends on several metrics that approximate ease of exploit and the impact of exploit. Scores are calculated based on the metric values each carrying a set of formulas for the impact of exploit. Scores may vary from 0 to 10, where 10 have the maximum chances for vulnerability. Here the CVSS system is used to analyze the vulnerability in a power grid using the three metric values [8] [10]...

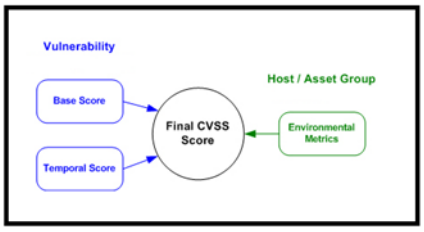

Fig. (1) Influence of the metric values

With respect to the metric values the following assumptions are made, the data in a power grid is stored in form of tables. Therefore the vulnerability occurs as follows. A vulnerability in the Server database could allow a remote, insider to inject threats into the database with high privileges. After math effects of the injections are very hazardous as the insider may delete or modify the data in the My SQL server [11].

A. Base Metrices

Fig. (2) Base Score

As mentioned in the figure fig. (2) The metric values are as follows: Attack Vector (AV) (Network (N)) this vulnerability means the insider has the access through the network, OSI layer 3 (the network layer). The data in the network with low firewall can be accessed in one or many ways. Such vulnerabilities are termed as remotely exploitable. For example, a Denial of Service (DoS) attack caused by an attacker from a public internet by sending specially crafted TCP crafted packets. Attack Complexity (AC) (H-High)Executing attack effectively based on the rules apart from the attackers rules. Privileges Required (PR) (L- Low) Certain freedoms are using by the attacker to get authorization that give them access only to certain interactions on to the databases. On the other hand, the attacker with least privileges has access only to the least sensible data. User Interaction (UI) (N- None) - Susceptible system is not permitted to access for any users for any communication. Scope (S) (Unchanged (U)) The resources managed by the same authority has the exploited vulnerability. Here, affected component and weakness component both are same. Confidentiality Impact (C) (High (H))whole damage of privacy is caused, whenever the chance is created to reach all resources within the component to attacker. Though the information is presented with a direct and serious impact. Integrity (I) (High (H)) this leads to a complete damage in protection or whole damage in integrity. For example, secured files are partially or completely can be altered by the attacker. These modifications may seem to be negligible but it causes a very serious impact onto the overall data that has been protected. Availability (A) (Low (L)) The resource availability has only reduced performance in the entire database server. Component of the database is available as partially at any time or completely available for short time. However generally direct is not possible

for any specific component of the database [13].

B. Temporal Metrices

Fig. (3) Temporal Score

As mentioned in the fig. (3) The metric values are as follows: Exploit Code Maturity (E) (Serviceable (F)) Serviceable features are made obtainable directly to anyone of power grid. If the vulnerability level persists, then the code may get executed. Remediation Level (RL) (Official Fix (O)) - An authenticated users can get the entire solution of the hawker in the power grid. The vendor should make the official patch available to the authenticated user in the power grids. Report Confidence (RC) (Confirmed (C)) - Detailed reports should be prevented from the insider threats, as it gives them the source to access all the details from the power grids. This report confidence should summarize all the necessary details of the power grids [13].

C. Environmental Metrices

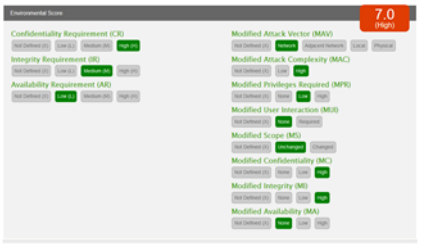

Fig. (4) Environmental Score

The Environmental metric group represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

The Environmental metrics are specified by end-user organizations because they are best able to assess the potential impact of a

vulnerability within their own computing environment. Although, the privacy necessity is increasing that is considered to be highly defensive which is not changing the score values if it is changed from Medium to high. The impact sub score possess the maximum value of 10 which does not reflect with any changes in the environmental Metrics or scores that are given. The mitigations are given to the environmental metrics. Often modified metrics are used to define the base metric values [12] [13].

5 QUALITATIVE SEVERITY RATING SCALE

A textual representation is highly recommended for the use of Base metrics, Temporal metrics and Environmental metrics. These scores are directly mapped to the qualitative ratings for the better understanding [12] [10].

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Table.1

And thus the vulnerabilities are analyzed for the power grid.

6 Conclusion:

From the common vulnerability scoring system (cvss) we can get the vulnerability of the power system with which we give the suitable security to the power system based on the CVSS score.

References

[1] Yi Zhou , Zhixin Mia, Cyber Attack Detection and Protection in smart grid State Estimation , IEEE Xplore: November 2016.

[2] Zacl De Smit , Ahmad E. Elhalsashy , Lee .well. An Approach to cyber- physical Vulnerability assessment for intelligent Manufacturing Systems Journal of Manufacturing Systems Volume 43, part 2 ,pp. 339-351, April 2007

[3] Chee-Wooi Ten ,Vulnerability Assessment of Cyber security for SCADA Systems, IEEE Transaction on Power Systems Volume: 23, Issue: 4, Nov. 2008

[4] Acs publications Cyber Security Threats Challenges, Opportunities, November 2016.

[5] Chih-Che Sun , Chen-Ching Liu and Jing Xie , Cyber-Physical System Security of a Power Grid: State-of-the-Art,July 2016

[6] US NRC- United Nations Nuclear Regulatory Commission, Protecting the People and Environment.

[7] Zhenhua Yu, Lijun Zhou,Trustworthiness Modelling and Analysis of Cyber- Physical Manufacturing SystemsIEEE Acces(Volume:5) pp: 26076 26085,Novemeber 2017.

[8] Leonid Stoimenov , Milos Bogdanovic and Sanja Bogdanovic-DinicESB-Based Sensor Web Integration for the Prediction of Electric Power Supply System Vulnerability August 2013.

[9] Haibo He, Jun YanCyber-physical attacks and defences in the smart grid: a survey.

[10] John T Chambers,Common Vulnerability Scoring System October 2004.

[11] Assad Ali, Pavol Zavarsky,A Software Application to analyse the effects of temporal and environmental metrics on overall CSVV v2 score IEEE explore 15 April 2011

[12] Laurent Gallon"On Impact of Environmental Metrics on CVSS Score" IEEE explore 2010 Technology & Computer Science at the BA-University of Cooperative Education, ITCS 2005.

[13] www.first.org/cvss