ORIGINAL RESEARCH PAPER
Volume - 11 | Issue - 05 | May - 2022 | PRINT ISSN No. 2277 - 8179 | DOI : 10.36106/ijsr
INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH

A CYBERSECURITY ANALYSIS MODEL OF CALIBRATION SOFTWARE FOR VULNERABILITY ASSESSMENT.

Computer Science

Nishanth Shanmugam M.Tech Computer Science and Engineering Student, Department of Computer Science and Engineering, Government College of Engineering Aurangabad, Maharashtra, India 431005.

Prashant Pathak* Assistant Professor, Department of Computer Science and Engineering, Government College of Engineering Aurangabad, Maharashtra, India. *Corresponding Author

ABSTRACT

Cybersecurity is one of the crucial factors in web application success. Nowadays, with the rise in cyber attacks users expect a safe environment. To meet that expectation, our goal was to assess the security preparedness of the Calibration software. The calibration software is a web-based calibration management tool that helps you maintain and control your calibration environment. Also, manage the calibration of all measurement devices for the specified business location and set up a calibration work schedule for technicians. We propose a cybersecurity analysis algorithm using the Policy Analyser (LGPO), Zed Attack Proxy, NESSUS, Network Mapper, Attack Surface Analyser, and SigCheck tool to perform a security risk assessment. We argue that the security of calibration software can be significantly increased. In this study, we have described our approach to security analysis and measuring their safety and presented our results.

KEYWORDS

Security Analysis, Network Security, Calibration Software, Vulnerability

INTRODUCTION

This is the next-generation calibration and asset management software that provides full visibility of all assets, references standards, and plant resources. This software effectively integrates people with the company's pressure calibrators and controllers to provide a holistic calibration solution. It works easily and safely, effective maintenance while helping to manage the process by enhancing the process efficiency and avoidance of human errors. The web browser-based design of calibration software allows you to access data anytime, anywhere eliminating the need to maintain and manage paper-based records.

A. Maintaining Simple, Smart, Scalable

Calibration software offers the flexibility you need - calibration management software that can be used from a separate computer or shortened to network solutions is a web-based architecture that allows users to simply log in to a web browser from any location.

With the server's integrated communications package, you can easily download and install it to interact with your devices. Calibration software reduces calibration time and provides automation and integration capabilities cost once installed, it can be easily calculated for a large number of users or devices to meet your growing calibration needs.

B. Compliant and audit-ready

It offers paperless, automated workload schedules and management, extensive control over calibration workflow and data, easy access to historical calibrations, and the ability to generate reports in customized formats. Regulatory compliance can also be given with this calibration software uncertainty calculation feature able to reverse trace calibrations for further peace of mind.

C. Calibration made smart

This allows the functionality of the historical trending module assets for maintenance from time to time. Calibration software provides strong solutions to error analysis and historical trending. Then understand the deviations and errors used to apply the correct procedure corrective action and preventive action (CAPA) to reduce calibration errors improving quality.

LITERATURE SURVEY

A. The traditional calibration process

The 8-step process highlights the traditional, paper-based calibration process. This is highly inefficient, labor-intensive, and involves manual data storage which is time-consuming and error-prone.

Less Efficient - The 8-step process takes over 2 hours to complete, due to the intensive preparation and verification of results required.

B. The new improved calibration process

By utilizing the Calibration and Asset management software, to automate the calibration process and remove the need for manual data entry and storage, your process can be more efficient, saving you time and money.

Figure 1: Calibration in progress

Sources: www.googleimages.com/calibration

OBJECTIVE / STATEMENT OF PROBLEM

Main Objective - Analyse Calibration Management Software application to improve product safety and address security issues.

Further Objectives are divided into 3 steps:

1) To understand the basic concepts of security analysis and calibration.

2) To implement enhancements and security tests.

3) To analyze and evaluate the safety and security of the proposed system.

METHODOLOGY

Cybersecurity analysis is a type of software security analysis that ensures system applications perform securely under their expected workload in any network. It runs security tools to determine system security in course of expected usage. There are 6 stages in security analysis for a calibration software project, as shown in figure 2.

A. Analyze the existing environments

In the existing environment, the local policies and cybersecurity configurations are understood. The effectiveness of the policies and configurations in the current environment have to be analyzed.

B. Gather security configurations of the current system

Gathered all required information about security and the policies present in the software need to be checked.

C. Define the analysis model and implementation of the algorithm

The security analysis algorithm implementation-defined as shown in

the below figure. Policy Analyser, Zed Attack Proxy, NESSUS, Nmap, and Attack Surface Analyser followed by Signature Check are the major components of the cybersecurity analysis flow.

D. Define the security analysis acceptance criteria

As per the above flow, the calibration software was securely tested along with baseline and post-scan analysis. Low vulnerability issues could be accepted. Medium and High vulnerabilities such as OpenSSL were immediately reported & rectified.

E. Configure the security test environments

In the software system, we have analyzed the baseline policies, network, and software configurations before proceeding with security analysis. LGPO tracked the policy changes and the network mapper provided network changes after running scan post-attack scenarios.

F. Execute planned scenarios

Executed the security scans and tests in calibration software in the following order – LGPO Policy Analyser, Zed Attack Proxy, NESSUS, Network Mapper, Attack Surface Analyser with baseline and post-scan report generation followed by SigCheck to verify the signature of installed software files.

G. Monitor web server, application server, and database server's security compliance

Monitoring the application and database server from the following-ing things – Network Mapping (Port Handling), NESSUS for logging vulnerabilities while software use and categorizing into low, medium, and high priority, followed by Attack Surface Analyser for policy comparison and changes post-installation or feature use and lastly signature check for verification of installed file binaries.

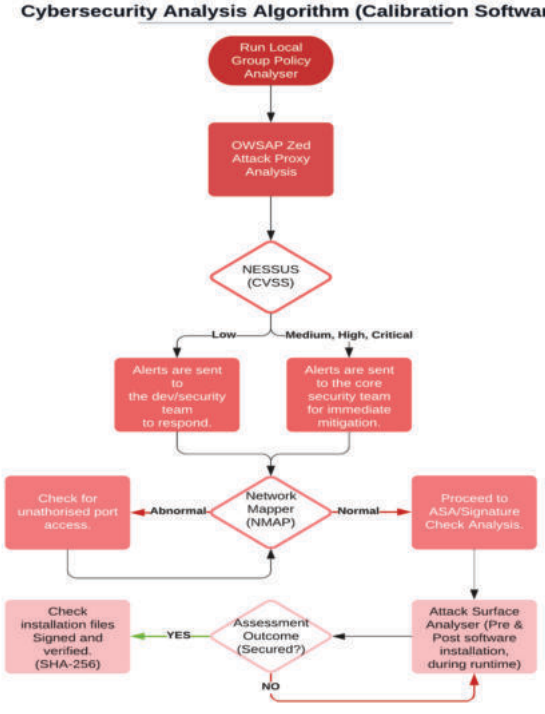

Fig 2. Proposed Cybersecurity Analysis Algorithm for Calibration Software

F. Correlate and analyze the results

Studied the cybersecurity findings and analyzed the results. From the results, we understand whether our system runs securely or not.

G. Provide security improvement recommendations

We provided the recommendations on basis of the results that we obtained from the security analysis to further strengthen the group policies and software feature developments to ensure the best security.

RESULT

According to the cybersecurity assessment model the software system was found to satisfy the model acceptance criteria as shown in below results table.

Cybersecurity Assesment	Result Achieved	Percent Match (Security Fulfillment)	Within Cybersecurity Model Acceptance (Yes/No)
Local Group Policy Analyser	1. Baseline with Group Object IDs and Security Policies. 2. Final (Post Analysis) with Object IDs and Modified Security Policies.	100%	Yes
Zed Attack Proxy (ZAP)	1. Generate Alert Counts. 2. Alert Level defined by Risk & Confidence Matrix (Types - Low, Medium, High, Informational). 3. Absence of Anti-CSRF Tokens, Error Disclosure, Debug, X-Content-Type-Options Header Missing.	98%	Yes
NESSUS	1. Critical (0), High (0), Medium (5), Low (2), Informational (30) Risk Assessment performed and result obtained. (Pre & Post Software Installation). 2. SSL (SWEET32), TLS Version, DCE Services Enumeration, RDP Identification, SMB Signing vulnerabilities detected and security patched.	90%	Yes
NMAP	1. 1 Host and Target IP assessed. 2. Network Distance: 0/0 Hops TCP Sequence Prediction: Difficulty=256 (Level) IP ID Sequence Generation: Incremental Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows Raw Packets Sent : 65616 (2.891 MB) | Received : 140922 (6.067MB)	100%	Yes
Attack Surface Analyser (ASA)	1. Base and Post JSON Analysis. 2. Parameters include SID, Password Privileges, BaseRunID, Domain, CompareRunID 3. All parameters have matched before and post product installation	100%	Yes
Signature Check	1. Binary checks on all installed files contains 256-bit digital signature. 2. Classified as Signed or Unsigned. 3. Verified from Apache Software Foundation, Amazon, OpenJDK.	100%	Yes

CONCLUSION

Cybersecurity assessment has always been a major challenge for developers and QA Engineers. In this study, we proposed and demonstrated real-time instructions exploring the ability to use LGPO Policy Analyser, Zed Attack Proxy, NESSUS, Network Mapper, Attack Surface Analyser, and SigCheck on our calibration software. The security of this web application is critical to be analyzed to ensure its optimal and safe functioning in real-time situations. By analyzing the security aspects, many important features or lapses may have come to the fore in the early stages of the software development cycle and usage. This saves a lot of time and resources post the proposed procedures as software distribution becomes easy to deploy and learn, hence minimal human intervention is required. In addition, they can contribute to calibration safety and show security improvements. This will be an important resource for security enhancements and software design.

REFERENCES:

[1] DeSmit, Z., Elhabashy, A. E., Wells, L. J., & Camelio, J. A. (2016). Cyber-physical vulnerability assessment in manufacturing systems. Procedia Manufacturing, 5, 1060–1074. https://doi.org/10.1016/j.promfg.2016.08.075

[2] Roldán-Molina, G., Almache-Cueva, M., Silva-Rabadão, C., Yevseyeva, I., & Basto-Fernandes, V. (2017). A Comparison of Cybersecurity Risk Analysis Tools. Procedia Computer Science, 121, 568–575. https://doi.org/10.1016/j.procs.2017.11.075

[3] Oughton, E. J., Ralph, D., Pant, R., Leverett, E., Copic, J., Thacker, S., ... & Hall, J. W. (2019). Stochastic counterfactual risk analysis for the vulnerability assessment of cyber-physical attacks on electricity distribution infrastructure networks. Risk Analysis, 39(9), 2012-2031.

[4] Jauhar, S., Chen, B., Temple, W. G., Dong, X., Kalbarczyk, Z., Sanders, W. H., & Nicol, D. M. (2015, November). Model-based cybersecurity assessment with nescor smart grid failure scenarios. In 2015 IEEE 21st Pacific Rim international symposium on dependable computing (PRDC) (pp. 319-324). IEEE.

[5] Gourisetti, N. G., Mylrea, M., & Patangia, H. (2019, January). Application of rank-weight methods to blockchain cybersecurity vulnerability assessment framework. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0206-0213). IEEE.

[6] Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2019). Cyber security management model for critical infrastructure.

[7] Shah, S., & Mehtre, B. M. (2013). A modern approach to cyber security analysis using vulnerability assessment and penetration testing. Int J Electron Commun Comput Eng, 4(6), 47-52.