An Evaluation of Security Posture Assessment Tools on a SCADA Environment

Shahir Majed¹, Suhaimi Ibrahim¹, Mohamed Shaaban²
¹Advance Informatics School, Universiti Teknologi Malaysia, International Campus, Jalan Semarak 54100 Kuala Lumpur Malaysia
shahir.majed@mimos.my, suhaimiibrahim@utm.my
²Centre of Electrical Energy Systems (CEES)
Faculty of Electrical Engineering
Universiti Teknologi Malaysia
m.shaaban@fke.utm.my

Abstract—Increased concerns for energy grid cybersecurity has lead to the development of compliance requirements that must be evaluated by utilities. The North American Electric Reliability Council (NERC) has created Critical Infrastructure Protection (CIP) requirements for all cyber assets supporting the bulk energy system [17]. This research explores whether the methodologies and tools commonly used for traditional information technology (IT) systems are sufficient to meet the cybersecurity assessment needs in power systems. This paper reviews these assessment tools to determine their ability to assist in the evaluation of the CIP requirements. In addition to the evaluation the tool capabilities, they are also reviewed for their potential to negatively impact the network availability properties. Evaluation was performed on the SecureCyber testbed at MIMOS & UTM -AIS Lab which implements real-world environment as in employs industry standard hardware, software and field devices. The result of this analysis is provided along with a review known gaps where current IT cybersecurity tools do not appropriately support SCADA environments.

I. INTRODUCTION

While cyber vulnerability assessments have become a standardized process in information technology (IT), they have only recently gained importance in SCADA environments. Demand from the IT side has driven the development of evaluation tools, test methodologies, impact scoring and reporting procedures to assist with the reliability and efficiency of the assessment process. The similarities between traditional IT and SCADA systems should ensure a portion of IT assessment methods have some applicability to SCADA environments.

This paper documents the results from an evaluation of whether current techniques for vulnerability assessments provide appropriate coverage of SCADA assessments. The evaluation of current IT assessment tools will be reviewed on the MIMOS-UTM SecureCyber testbed. These analyses will specifically targeting their ability to evaluate IEC61850 compliance. In addition, these tools will be analyzed to detect potential negative affects the assessment may have on network availability.

II. PREVIOUS WORK

The evaluation of cyber vulnerabilities in control systems has been a popular area of recent research. Center of Smart Grid Systems at MIMOS has establish the National SCADA Testbed (NSTB) which provides a resource to evaluate critical vulnerabilities in realistic SCADA systems.[14] MIMOS has provided research documenting cyber vulnerabilities commonly found in SCADA systems and has also provided an overview of tools and techniques utilizes to perform this analysis.[11][9][15]. Research at Sandia National Laboratory has provided guidance on performing a
cyber vulnerability assessment on an SCADA system. [19] Additional work has addressed concerns for performing penetrations tests on control systems.[12] This research differentiates itself from the previous works as it applies techniques from a cybersecurity assessment methodology to a SCADA testbed utilizing known tools commonly used in traditional IT assessments to simulate the assessment capabilities of current utilities.

A. Testbed Architecture

The SecureCyber testbed was developed at UTM AIS to provide a realistic SCADA system for cyber vulnerability evaluation.[13] The testbed utilizes real-world hardware and software to provide an accurate representation of a SCADA system. The components contained in the testbed include human-machine interfaces (HMIs), SCADA servers, remote terminal units (RTUs), overcurrent protection relays, historian servers and virtual private network (VPN) devices. The HMI provides the operator with an interface to the SCADA server. This is utilized to perform monitoring and control of the system operations. The SCADA server communicates with the RTUs in the appropriate substations and relays commands from the HMI. The RTU provides a centralized system within a substation to communicate with various intelligent electronic devices (IEDs), such as the relays.

The testbed architecture, as displayed in figure 1, shows the layout of the control center and two substations. The control center contains the HMI, SCADA server, and historian server. Each substation contains a RTU which is connected to a relay. Communication between the control center and substation is protected with the VPN devices provide which a secure channel.

The SCADA specific protocols in use are DNP3 and IEC 61850. DNP3 is a protocol primarily intended for the communication of a variety of different process control system. In the testbed DNP3 is used to transmit the data points between the RTUs and SCADA server. The IEC 61850 protocol is highly specialized towards substations and, therefore, is used for communication between the RTU and relays. The network is implemented on an Ethernet network and all communications utilize TCP/IP.

Techniques used to evaluate the current cybersecurity posture can vary based on requirements and goals. Often these techniques combine reviews of technical security controls and non-technical policies, procedures and documentation. This section will review current cybersecurity evaluation methods to determine their applicability to SCADA environments.

A. Compliance Requirements

An important objective for a cybersecurity assessment methodology is the ability to determine whether compliance requirements have been sufficiently meet. Since SCADA systems supporting the bulk power system are required to be IEC 61850 compliant, an effective SCADA test methodology must evaluate each individual requirement. A review of the IEC 61850 standards was performed to determine technical security requirements which must be addressed by SCADA assessment.
methodologies. A table documenting the relevant technical security controls is provided in figure 2.

B. Assessment Methodologies

The scope of assessment activities is dependent on the test methodology. A thorough methodology is imperative to ensure that all required evaluations are performed consistently. Before reviewing various methodologies we first review the different assessment types.

Technical security evaluations are often categorized as either vulnerability assessments or penetration tests. While both share common techniques, there are significant differences in how they are performed and their impact on the target systems. Vulnerability assessments are an evaluation of technical vulnerabilities in a system. Vulnerability assessments are typically performed as white-box tests where testers have access to documentation, configurations and personnel in order to obtain a full understanding of all potential security weaknesses. During a vulnerability assessment security concerns are documented, but no exploitation occurs. Penetration testing involves attempts to exploit weaknesses to validate its severity and determine the feasibility of a cyber attack. Since penetration tests involve attempts to bypass security controls they are more likely to negatively impact system availability. From a SCADA perspective, vulnerability assessments will typically be preferred as they provide a comprehensive review of the security posture. In addition, it is generally not recommended to perform penetration testing on production SCADA systems.

Assessment methodologies can employ varying breadth and depth of analysis. Some notable methodologies from traditional IT are displayed below.

- NIST SP 800-53A, Guide for Assessing the Security

This research primarily utilizes a slight modification to the methodology provided by NIST SP 800-115 because it is publicly available and also references other methodologies. NIST 800-115 provides a comprehensive review of the vulnerability assessment process including coordination, planning, technical and non-technical analysis, data handling and reporting. In addition, it suggests additional resources that may be helpful when performing an assessment such as software tools, vulnerability sources and additional documentation. Figure 3 documents the assessment steps performed in this assessment, note they essentially follow those documented in NIST 800-115 except for potentially disruptive system penetration activities.

IV. ASSESSMENT RESULTS

The section will address the various evaluation activities in further detail and document cybersecurity evaluation tools used to perform this analysis. This specifically addresses two concerns, first, whether the assessment tool was able to achieve

| CIP-002-3 Critical Cyber Asset Identification | R1.1 | “documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria” |
| CIP-003-3 Security Management Controls | R5.2 | R5.2 "at least annually the access privileges to protected information to confirm that access privileges are correct” |
| CIP-005-2a Electronic Security Perimeters | R2.1 | “use an access control model that denies access by default” |
| | R2.2 | “enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic” |
| | R2.3 | “maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s)” |
| | R.26 | “display an appropriate use banner on the user screen upon all interactive access attempts” |
### CIP-007-2a System Security Management

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1.1</td>
<td>“create, implement, and maintain cyber security test procedures”</td>
</tr>
<tr>
<td>R2</td>
<td>“implement process to ensure that only those ports and services required for normal emergency operations are enabled”</td>
</tr>
<tr>
<td></td>
<td>“assessment of security patches and security upgrades for applicability within thirty calendar days of availability”</td>
</tr>
<tr>
<td>R3.1</td>
<td>“implement a process for the update of anti-virus and malware prevention signatures. The process must address testing and installing the signatures.”</td>
</tr>
<tr>
<td>R4.2</td>
<td>“assessment of security patches and security upgrades for applicability within thirty calendar days of availability”</td>
</tr>
<tr>
<td>R5</td>
<td>“establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity”</td>
</tr>
<tr>
<td>R5.1.3</td>
<td>“review, at least annually, user accounts to verify access privileges”</td>
</tr>
<tr>
<td>R5.3</td>
<td>“require and use passwords, subject to the following”, “six characters”, “combination of alpha, numeric and special characters” and “changed at least annually”</td>
</tr>
<tr>
<td>R6.3</td>
<td>“maintain logs of system events related to cybersecurity”</td>
</tr>
<tr>
<td>R6.4</td>
<td>“retain all logs specified in Requirement R6 for ninety calendar days”</td>
</tr>
<tr>
<td></td>
<td>“review of controls for default accounts”</td>
</tr>
</tbody>
</table>

---

**Fig. 2. NERC CIP statements requiring technical cybersecurity assessment[17]**

**Fig. 3. Assessment Methodology**

The required function from the NIST 800-115 methodology and second, whether the tool was sufficient to evaluate NERC CIP requirements. Any data pertaining to potential vulnerabilities and other security weaknesses is not included to avoid exposing sensitive information.

#### A. Network Traffic Review

The review of network traffic is required to gain a thorough understanding of the network communication. This technique does not involve sending any additional network traffic and therefore should not negatively impact network reliability. The review of network traffic provides the tester with an understanding of what network services are being accessed and what data is being passed through the network. This information is useful when doing later vulnerability scanning and also enables the inspection of authentication and encryption mechanisms used in the network. Wireshark is currently the industry standard tool for traffic review.[8] This tool provides protocol dissection capability, meaning that it parses out and displays known fields from the network traffic to provide the user with more meaningful information. Wireshark provides support for many common SCADA protocols including Fieldbus/Modbus, OPC, DNP3, GOOSE, IEC 60870-5-104, and IEEE C37.118.

During the assessment Wireshark was only able to inspect a subset of the system’s communications. Since the testbed utilizes both DNP3 and GOOSE, as a subset of IEC 61850, Wireshark was able to provide useful information about these communications. Unfortunately there appeared to be numerous communications employing proprietary protocols which Wireshark was unable to identify. This leaves open questions about the criticality of these communications.

#### B. System Configuration Review

The review of a system’s configuration is dependent on knowledge of known security issues within the software and current best practice. While there are well documented security baselines for many popular IT software products[7], most SCADA software has not undergone comparable analysis. This provides a unique challenge when performing a cyber vulnerability assessment. While some vendor specific guidance may be provided it may not be centrally collected for easy review. Therefore, testers...
have a limited ability to verify security related configurations in SCADA software.

Often automated tools are available to evaluate the configurations of popular IT software products. The Open Vulnerability Assessment Language (OVAL) Interpreter is one software tool that can perform this security baseline evaluation. The results of running the OVAL Interpreter on the SCADA stations resulted in over one hundred potential mis-configuration. Unfortunately, many of the recommended configurations do not map well to the SCADA domain as they may negatively affect system availability. Potentially problematic settings could include password/account lockout policies, unprotected Windows shares, or disabled automatic system updates. Therefore, even with the utilization of the OVAL Interpreter our analysis was not able to determine an optimal system configuration.

C. Network Discovery, Port and Protocol Identification

Although information about network host and communication protocols should be well known by the network administrators, the discovery process is necessary to validate any assumptions. Network discovery is often performed with a port scanning tool such as Nmap.[5] Nmap work by sending packets to all TCP and UDP ports in an attempt to determine what services are running on the network. It can also be used to send ICMP echo request (ping) packets to all systems on a network in order to determine all connected systems. In addition to discovery and port identification, Nmap also provides the ability to analyze protocols based on common port number matching as well as the ability to correlation the server responses against known protocol fingerprints.

During the assessment Nmap was able to identify all systems through an ICMP scan. However, this network may not be accurately represent other SCADA environments due to its small size and homogeneous network structure. In other cases Nmap may not appropriate identify all systems in networks with packet filtering firewalls or non-TCP/IP network segments. Additional tools such as Sandia’s ANTFARM may be necessary to perform this evaluation.[1]

Nmap was also utilized effectively to evaluate all open TCP and UDP ports. While all open ports were determined, Nmap was not able to identify 53 out of 157 the open ports utilized in the network. This occurrence is a result of the heavy utilization of proprietary and SCADA specific protocols which are not recognized by Nmap. This indicates that additional inspection is required to determine the protocols used in the environment.

D. Vulnerability Scanning

Vulnerability scanning typically encompasses various network identification techniques to determine potential security concerns in various software. Often special assessment tools provide a centralized ability to perform a comprehensive analysis of known security vulnerabilities characteristics in order to detect potential vulnerabilities. The Tenable Nessus Network Security Scanner is a commercial vulnerability scanner which has traditional provided support of only traditional IT software.[4] Recently security vulnerabilities for certain SCADA platforms
have been added to Nessus, though support for SCADA platforms is still limited.

Nessus scans were performed against all systems. The result provides a range of medium and low findings which primarily addressed the configuration best practice and system patching issues. No SCADA specific vulnerabilities were identified by this analysis. This occurrence could either be explained by the lack of known vulnerabilities or a lack of support for the specific software utilized in the testbed.

V. COMPLIANCE EVALUATION

While the previous section reviewed the applicability of various assessment tools to a SCADA environment it did not address the evaluation of IEC 61850 standards. This section utilizes the previous results to determine how well the tools appropriately cover the IEC 61850 requirements. Figure 4 documents whether the tools used during this assessment have the ability to evaluate whether the CIP security controls listed in figure 2. Open circles indicate that the tool does not inspect the requirement, half full circles indicate partial inspection, and full circles indicate that the tools is sufficient to meet this objective. In order to correlate tools with their corresponding objectives in the assessment methodology the following numbers are referenced in the figure.

1) System Configuration Review
2) Network Traffic Review
3) Network Rulesets Review
4) Network Discovery
5) Port/Protocol Identification
6) Vulnerability Scanning

Figure 4 shows that evaluating NERC CIP requirements will require additional tools along with some manual system inspection. Certain requirements R2.6 in standard CIP 005-2a and R5.1.3 from standard CIP 007-2a may vary greatly between systems and will likely require human analysis. Effective evaluation of requirements R6.3 and R6.4 from standard CIP 007-2a should determine whether a log correlation mechanism is collecting and aggregating logs from multiple systems. Assessment methods should analyze the effectiveness of these tools.

VI. GAP ANALYSIS

The evaluation of current cybersecurity assessment tools has provided some concerns in areas where additional research is required. This section will address gaps that have been found while performing the previous assessment due to differences in IT and SCADA environments.

A. Unknown Protocols

The testbed software was found to rely heavily on proprietary network protocols. These protocols were not identified by any analysis tools due to the combination of unusual TCP/UDP ports and undetectable network protocols. The utilization of proprietary protocols and lack of appropriate protocol dissectors limited our ability to identify the network communication. Without this understanding it is difficult to determine the controls required to appropriately secure the communication.

B. Undocumented Software Versions

During our assessment we found that the SCADA systems leveraged a number of undocumented software packages. This information was only determined after a detailed inspection and could be easily overlooked during more routine inspection. Vendors often utilize other commercial or open source programs within their larger software packages. Any security concerns with third-party tools may be well understood since the software is likely used in other industries. A security tester that is unable to determine all third-party software may overlook critical vulnerabilities.

C. Unknown Configuration Requirements

The security assessment provided two concerns with the lack of documentation addressing appropriate configurations. First, there was insufficient documentation on how the SCADA software should be securely configured. While the documentation had some security related information, it was not centralized to ensure it could be reviewed in a reasonable timeframe. Second, since the SCADA
software operates on Microsoft Windows Operating Systems, known Windows security configurations cannot be applied without affecting SCADA reliability. Therefore, security relevant configurations cannot be confidently implemented.

D. System Availability

System availability provides an additional concern when performing a cybersecurity evaluation. Heavy availability requirements will limit the use of any methods which could result in system faults. During the assessment it was determined that certain testing methods were able to initiate system failures. Specifically, a port scan of certain systems was sufficient to cause a software failure cause the system to crash. While only one failure was found during the evaluation, the situation provides concerns for stability of the system during an assessment. Fortunately CIP R1.2 allows the assessment on non-productions systems as long as the test environment. This is practice is heavily recommended as other SCADA platforms may be less resilient than the one tested in this environment. However, ensuring the consistency between the test and production environment requires the implementation of a thorough configuration management process to ensure all current configurations are appropriately documented.

VII. CONCLUSIONS

The need to perform cyber vulnerability assessments is becoming increasingly important. While techniques and methodologies have been thoroughly researched in IT, their applicability to power systems remains unestablished. This paper has reviewed common IT assessment techniques on a SCADA testbed and evaluated their ability to meet current security requirements; specifically those implemented by IEC 61850 standards. The results of these assessment methods are then documented, specifically identifying areas where current IT assessment methods do not appropriately transfer into the SCADA systems. During our assessment we found availability concerns in the SCADA platform which reinforce concerns for performing assessments on production environments.

This conclusion provides rational for assessment methods which are more effective and less intrusive. While the current capabilities to perform SCADA cyber vulnerability assessments are limited, recent advancements in IT security evaluation tools may provide a significant addition. The NIST Security Content Automation Protocol (SCAP) introduces a standardized format for evaluating the security posture of a system. SCAP provides a standard baseline for a system’s security relevant parameters which can be used to express checklists of known security system states.[18] These checklists can be utilized by SCAP-compliant security assessment tools to evaluate system configuration.

Performing a SCAP compliant assessment typically involves authenticating to a system and evaluating the current configurations. This method does not depend on intrusive network scanning which has shown to cause system faults. In addition to SCAP, the DOE sponsored Bandolier project by Digital Bond provides assessment specifications for certain common SCADA software platforms.[2] Bandolier provides these specifications as a commercial set of Nessus audit files tailored to inspect the these implementations. Nessus can then utilize these specifications to evaluate SCADA configurations without impacting system availability. Tools like SCAP and Bandolier provide important research avenues in the SCADA cyber vulnerability assessment domain.

ACKNOWLEDGEMENT

"This research is funded by the Research University grant of Universiti Teknologi Malaysia (UTM) under the Vot no. 08H28. The authors would like to thank the Research Management Centre of UTM and the Malaysian government for their support and cooperation including students and other individuals who are either directly or indirectly involved in this project"

REFERENCES


