SUGISAKA MASANORI

Journal of Robotics, Networking and Artificial Life
Vol. 11(1); June (2024), pp. 11–15
ISSN (Online): 2352-6386; ISSN (Print): 2405-9021
https://alife-robotics.org/jrnal.html

Research Article

The Intrusion Detection Solution for Isolated Industrial Control Environments

I-Hsien Liu[1], Nai-Yu Chen[2], Pei-Wen Chou[2], Jung-Shian Li[3]

[1]*Department of Electrical Engineering, National Cheng Kung University, No.1, University Rd., East Dist., Tainan City 701401, Taiwan*
[2]*M.S. Degree Program on Cyber-Security Intelligence, National Cheng Kung University, No.1, University Rd., East Dist., Tainan City 701401, Taiwan*
[3]*Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University, No.1, University Rd., East Dist., Tainan City 701401, Taiwan*

ARTICLE INFO

Article History

Received 31 October 2023
Accepted 06 August 2024

Keywords

Network-based monitoring
Industrial control system
Cybersecurity testbed

ABSTRACT

This study explores the implementation of intrusion detection solutions, specifically Snort, in industrial control environments that use network segregation as a security measure. Unlike traditional deployments at gateway ports, our research integrates Snort directly within isolated networks, customized with specific operational technology (OT) rules. The effectiveness of this system was tested using the TWISC@NCKU Critical Infrastructure cybersecurity testbed in Taiwan. This findings indicate that this strategic approach can successfully detect anomalies in network traffic, effectively addressing the common challenge of limited monitoring in segregated network environments.

1. Introduction

Cybersecurity of critical infrastructure, is increasingly alarming, as recent significant incidents have demonstrated [1]. In December 2023, the Municipal Water Authority of Aliquippa (MWAA) in Pennsylvania was breached by hackers who took control of a booster station. These attackers, known as the Cyber Av3ngers, targeted the system because it used Unitronics equipment from Israel, consistent with their campaign against Israeli infrastructure. This example illustrates the vulnerabilities inherent in using specific brands of equipment and the geopolitical motivations that can drive cyber-attacks. Although this incident did not disrupt the water supply, it raised serious security concerns. The need for heightened vigilance and proactive measures to protect such vital infrastructure is evident.

In another noteworthy case from 2018, Aon and Guidewire Software released a report predicting a cyber-attack on American hydroelectric dams. This hypothetical scenario involved opening dam floodgates, potentially causing severe downstream flooding and major economic damage. The report highlighted the catastrophic potential of cyber-attacks on physical infrastructure, underlining the necessity for robust cyber defenses. The report emphasized the rising "silent cyber risk" to insurers, pointing out the largely uninsured nature of these cyber-physical threats, which could result in insurance claims of up to $10 billion, similar to losses from natural disasters like Hurricane Michael. The financial implications underscore the importance of integrating cybersecurity into risk management and insurance frameworks.

These incidents highlight the urgent need for strong cybersecurity measures in isolated network settings within ICS. While deploying an Intrusion Detection System (IDS) is a common strategy, the challenges are greater in environments lacking traditional network gateways, often seen in industrial settings [2]. Isolated networks pose unique challenges due to their limited connectivity and often outdated security protocols, necessitating tailored cybersecurity solutions. This study examines the implementation of a Network-Based monitoring mechanism to monitor and secure these isolated networks effectively [3]. Snort's adaptability makes it a suitable choice for customizing security measures to fit the specific needs of isolated ICS

Corresponding author E-mail: ihliu@cans.ee.ncku.edu.tw, nychen@cans.ee.ncku.edu.tw, pwchou@cans.ee.ncku.edu.tw, jsli@cans.ee.ncku.edu.tw
URL: www.ncku.edu.tw

networks. By customizing Snort to operate in these unique environments, our research aims to address monitoring gaps and enhance the security of critical infrastructures against advanced cyber threats. The goal is to provide a practical and scalable solution to protect vital industrial networks from sophisticated cyber-attacks.

2. Background

2.1. Purdue Enterprise Reference Architecture

Our study focuses on the cybersecurity of ICS by using the Purdue Enterprise Reference Architecture (PERA) as a framework [4]. Unlike typical ICS network designs, PERA omits traditional gateway components. This unique characteristic of PERA requires a thorough examination of how network isolation can be effectively implemented in environments that do not use standard network gateways. Our analysis reconsiders the relevance of establishing an Industrial Demilitarized Zone (IDMZ), particularly given the challenges of operating without conventional gateway infrastructure [5]. The research underscores the importance of deploying NIDS across critical layers of PERA to enhance security. NIDS monitor network traffic and detect suspicious activities, providing essential defense in ICS. By positioning NIDS within the PERA framework, we ensure comprehensive surveillance and effective threat mitigation.

Integrating PERA's architectural guidelines into our intrusion detection approach involves customizing NIDS for ICS networks, considering unique traffic patterns and operational protocols. This ensures effective detection of anomalies specific to industrial settings.

Our goal is to improve the resilience of industrial networks against cyber threats by deploying NIDS, implementing a comprehensive security strategy with regular updates, continuous monitoring, and effective incident response plans.

2.2. Attack Traffic Detection Methods

The importance of a Network-Based Intrusion Detection System (NIDS) is paramount in securing network traffic, particularly within ICS environments characterized by network isolation. A NIDS monitors network traffic for suspicious activity and potential threats, providing a critical layer of security by detecting and responding to intrusions in real-time. These systems are essential for maintaining constant surveillance and providing immediate alerts to any signs of intrusion. In isolated ICS environments, where traditional security measures might be insufficient, NIDS offers a way to continuously monitor and protect network integrity.

Based on this reason, we via a well-known open-source IDS solution, Snort, to customized with specific Operational Technology (OT) rules to fit isolated network contexts. Snort's versatility allows it to be tailored with OT-specific rules, making it suitable for the unique requirements of ICS networks. Snort's implementation in ICS takes advantage of its ability to perform both signature and rule-based detection, making it highly effective in identifying anomalies in network behavior. This flexibility enables Snort to be a critical component in strengthening security measures in environments with limited direct network connections. In such isolated environments, traditional network security measures are often inadequate, thus emphasizing the importance of a robust NIDS like Snort.

Using Snort in such scenarios not only enhances overall cybersecurity but also ensures strong protection against potential network intrusions. By providing real-time alerts and detailed logs of suspicious activities, Snort enables swift response and mitigation of threats, thereby securing critical infrastructure against cyber-attacks.

2.3. Internal ICS Attack Scenarios

In this research, we explore the functioning of NIDS within the isolated network settings of ICS. We focus on major security vulnerabilities, such as command injection and breaches of Integrated Development Environment (IDE) access [6], which threaten ICS operations.

Our study assesses attack types that target internal networks. Collaborating with TWISC@NCKU, we established a secure third-layer testing platform for control systems, crucial for overseeing dam operations through Human-Machine Interface (HMI). We identify methods of attacking sensors by injecting Modbus/TCP packets into Programmable Logic Controllers (PLCs). By concentrating on countermeasures against PLC shutdown attacks, we devise robust security enhancements to protect ICS against advanced network threats, offering effective strategies to strengthen critical infrastructure defenses in isolated network environments.

3. ICS Network Intrusion Detection Methods

Our study of NIDS in isolated ICS networks commenced with the integration of a Twido-developed HMI with the Programmable Logic Controller (PLC model TWDLCAE40DRF). To identify vulnerabilities,

we initiated a PLC shutdown and used Wireshark to capture the resulting Modbus protocol traffic. This was followed by the deployment of SNORT, which was precisely configured to meet the specific needs of an isolated ICS network.

Strategically positioning SNORT at the operational management layer was vital, as it utilized central database connectivity to link with HMI data visualization. The aim was to enhance the NIDS's capability to monitor this critical layer for intrusion signs.

The integration of NIDS with PLC communications was crucial, with a focus on identifying irregular network activities that could indicate a security breach. One of our main objectives was to evaluate Snort's effectiveness in isolated networks through a systematic approach (Fig. 1).

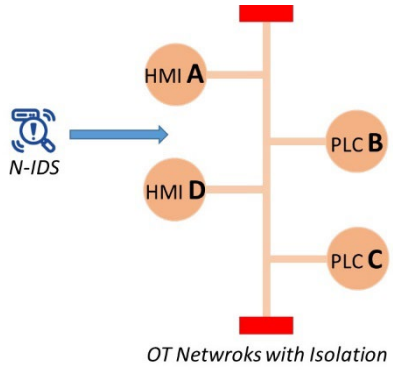

Fig. 1. NIDS, PLC, HMI Integration Architecture

Our research included creating specific SNORT rules to rapidly detect and neutralize malicious activities directed at PLC controllers [7] (Fig. 2). One of these rules was designed to analyze network traffic on Modbus port 502, searching for the '41FF00' hex data sequence, which is indicative of suspicious activity. This rule is a critical component of our strategy to identify and address immediate threats to PLC controllers, significantly enhancing the security framework of ICS networks.

```
alert tcp any any -> any 502 (msg:"Modbus/TCP Packe
Detected with '41ff00' Data"; content:"|00 00 00 00 00
06 ff 90|"; depth: 8; content:"41ff00"; sid:10000004;)
```

Fig. 2. Snort Rule for PLC Shutdown Detection

4. Experiment

We established a simulation environment and fine-tuned the parameters to emulate realistic cyberattack patterns on PLCs. We simulated PLC shutdown scenarios and monitored Modbus traffic anomalies using Wireshark. Snort was configured as the network intrusion detection system, specifically tailored with operational technology (OT) protocols [8]. The trials were conducted at the dam's gate control system one of the Critical Infrastructure cybersecurity testbed at TWISC@NCKU in Taiwan, ensuring the authenticity of the findings. Also explores the effectiveness of Snort in ICS environments with network isolation.

In this controlled setting, we conducted 30 individual trials, each lasting 20 minutes and including up to 20 attack simulations as described in Section 2.3. Standard HMI and PLC communications were maintained to ensure a realistic network traffic environment (Fig. 3). Our results showed that, on average, we identified 6.5 incidents of malicious activity out of 4560 packets per experiment, achieving a detection accuracy of 99.4%. These findings indicate a high probability—99.4%—of our system's ability to detect intrusions, highlighting the effectiveness of our security strategy.

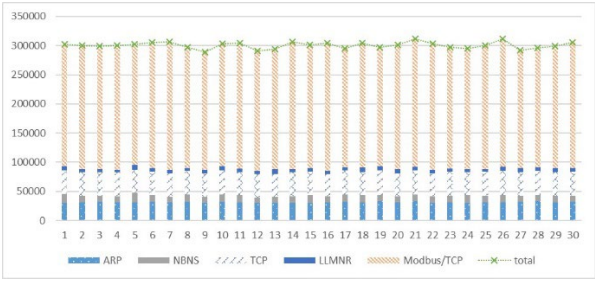

Fig. 3. Traffic Differences Among Various Protocols

5. Conclusion

This study focused on the integration of Network-Based Intrusion Detection Systems (NIDS), particularly Snort, into Industrial Control System (ICS) environments operating without direct gateway connections. These isolated networks present unique challenges for traditional intrusion detection due to the absence of gateway monitoring points. Through the TWISC@NCKU Critical Infrastructure cybersecurity testbed in Taiwan, to demonstrated Snort's ability to effectively identify irregular network behavior, addressing the issue of limited surveillance in these environments. This findings underline the adaptability and effectiveness of Snort in enhancing security measures for critical infrastructure, providing a practical solution to the monitoring gaps inherent in isolated networks.

This study improves network security measures within isolated ICS networks using intrusion detection methods customized to the specific needs of critical infrastructure. The integration of Snort with customized Operational Technology (OT) rules has shown to be a promising approach in detecting and mitigating cyber threats. The use of Snort in these contexts not only enhances real-time monitoring but also ensures a higher level of security resilience, adapting to the unique operational requirements of ICS environments.

Future investigations will expand upon this work by examining additional cyberattack scenarios. Given the limitations of our current setup, we plan to include an Engineering Working Station (EWS) and simulate standard IT threats to test the resilience of our methods. These enhancements will offer deeper insights into the strengths and weaknesses of intrusion detection systems in protecting ICS from various cyber threats. Furthermore, by expanding the scope of our testing environment to include more complex attack vectors and advanced threat models, we aim to refine our detection algorithms and improve the overall robustness of the system.

In addition to incorporating EWS, future work will also explore the integration of machine learning techniques to enhance anomaly detection capabilities. By leveraging data-driven models. This approach will contribute to the development of more proactive and adaptive cybersecurity strategies, ensuring that ICS environments remain secure against evolving threats.

Overall, this study lays the groundwork for a more secure and resilient approach to monitoring and protecting isolated ICS networks. By continually refining and testing our methods, we aim to provide a comprehensive and scalable solution that can be adapted to various industrial contexts, ultimately safeguarding critical infrastructure from potential cyber-attacks.

Acknowledgements

This work was supported by the Water Resources Agency (WRA) under the Ministry of Economic Affairs (MOEA) in Taiwan under contract number MOEAWRA1130243, and by the National Science and Technology Council (NSTC) in Taiwan under contract numbers 112-2634-F-006-001-MBK and 113-2634-F-006-001-MBK.

References

1. S.-G. Tân, I-H. Liu, J.-S. Li, "Simulation and Analysis of Common Attacks against PLCs Used in Dam Testbed," ARIS 2023, Taipei, Taiwan, 30 Aug. - 1 Sep. 2023.
2. G.-M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger and J. Benjamin, "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents," IEEE Access, vol. 9, pp. 165295-165325, 2021.
3. D. Zhang and J. Wang, "Research on Security Protection Method of Industrial Control Boundary Network," 2021 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS), Shenyang, China, 10-11 December 2021.
4. D. He, A. Lobov, L. E. G. Moctezumas and J. L. M. Lastra, "An approach to use PERA in Enterprise Modeling for industrial systems," IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society, Montreal, QC, Canada, 25-28 October 2012.
5. P. Ackerman, "Industrial Cybersecurity: Efficiently monitor the cybersecurity," posture of your ICS environment, Packt Publishing, 2021.
6. I-H. Liu, K.-M. Su and J.-S. Li, 2021, "The Security Issue of ICS: The Use of IT Infrastructure," Journal of Robotics, Networking and Artificial Life, 8(1), pp. 29-32.
7. E. R. Alphonsus and M. O. Abdullah, "A review on the applications of programmable logic controllers (PLCs)," Renewable and Sustainable Rnergy Reviews, Vol. 60, pp. 1185-1205, 2016
8. J. Luswata, P. Zavarsky, B. Swar and D. Zvabva, "Analysis of SCADA Security Using Penetration Testing: A Case Study on Modbus TCP Protocol," 2018 29th Biennial Symposium on Communications (BSC), Toronto, ON, Canada, 06-07 June 2018.

Authors Introduction

Dr. I-Hsien Liu

He is an assistant professor in Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his Ph.D. in 2015 in Computer and Communication Engineering from the National Cheng Kung University. He teaches cybersecurity courses and his interests are Cyber-Security, OT Security, and Wired & Wireless Communication. He is the deputy director of Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU).

Ms. Nai-Yu Chen

She is a postgraduate of M.S. Degree Program on Cyber-Security Intelligence, National Cheng Kung University in Taiwan. She received her B.B.A. degree from the Bachelor of BioBusiness Management, National Chiayi University, Taiwan in 2021. Her interests are ICS Security and Network-Based Intrusion.

Ms. Pei-Wen Chou

She is a postgraduate of M.S. Degree Program on Cyber-Security Intelligence, National Cheng Kung University in Taiwan. She received her B.B.A. degree from the Department of Healthcare Administration and Medical Informatics, Kaohsiung Medical University, Taiwan in 2022. Her interests encompass network security, blockchain, and industrial control systems.

Dr. Jung-Shian Li

He is a full Professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He graduated from the National Taiwan University, Taiwan, with B.S. in 1990 and M.S. degrees in 1992 in Electrical Engineering. He obtained his PhD in 1999 in Computer Science from the Technical University of Berlin, Germany. He teaches communication courses and his research interests include cybersecurity, cloud computing and network management. He is currently involved in funded research projects dealing with cybersecurity and critical infrastructure protection. He is the director of Taiwan Information Security Center @ National Cheng Kung University.