A Case Study of Network-Based Intrusion Detection System Deployment in Industrial Control Systems with Network Isolation

Nai-Yu Chen
Department of Electrical Engineering / Degree Program on Cyber-Security Intelligence, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

Pei-Wen Chou
Department of Electrical Engineering / Degree Program on Cyber-Security Intelligence, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

Jung-Shian Li
Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

I-Hsien Liu
Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan
*E- mail: nychen@cans.ee.ncku.edu.tw, pwchou@cans.ee.ncku.edu.tw, jsli@ cans.ee.ncku.edu.tw, ihliu@cans.ee.ncku.edu.tw**
www.ncku.edu.tw

Abstract

Deploying intrusion detection systems is a common cybersecurity measure, and intrusion detection systems typically operate at the ports of gateways. In critical infrastructure, industrial control systems often employ network isolation strategies, lacking the role of gateways. This research primarily explores the deployment of the Snort intrusion detection system in such an environment, combined with specific OT rules. Validation is conducted using the cybersecurity testbed of the dam control system established by TWISC@NCKU in Taiwan. The results indicate that by employing our proposed approach, it is possible to effectively detect abnormal network traffic, addressing the common issue of inadequate monitoring in environments with network isolation.

Keywords: Industrial Control Systems, Critical infrastructure, Network Isolation, Network-Based Intrusion Detection System

1. Introduction

The cybersecurity landscape in critical infrastructure, particularly Industrial Control Systems (ICS), faces escalating threats [1], exemplified by the recent CISA AA22-103A alert. This alert, prompted by internal ICS intrusion cases, underscores operators' vulnerability to targeted attacks, emphasizing the need for robust cybersecurity measures [2]. Deploying Intrusion Detection Systems (IDS) is standard, but challenges arise in ICS scenarios with network isolation policies.

This study delves into deploying Network-Based Intrusion Detection System (NIDS), focusing on the Snort intrusion detection system within network-isolated ICS [3]. Departing from conventional approaches, it addresses challenges posed by network isolation, offering nuanced network security tailored to ICS requirements. Snort, typically installed at gateway, assumes a novel role within network-isolated ICS. The research is motivated by the recognition that existing IDSs may fall short in effectively monitoring ICS within network isolation, prompting a reevaluation of intrusion detection strategies.

To validate the approach, this study leverages the TWISC@NCKU dam control systems cybersecurity testbed in Taiwan, providing insights into real-world applicability. The research's significance lies in addressing insufficient monitoring in network-isolated

environments. Developing Snort rules to detect "Close PLC Gate Controller" commands enhances ICS's capacity to defend against potential threats, fortifying critical infrastructure against evolving cyber threats. This introduction establishes the groundwork for exploring NIDS deployment in network-isolated ICSs, aiming to provide effective and tailored cybersecurity solutions for safeguarding ICSs.

2. Background

2.1. Isolation of Industrial Control Networks

This study explores ICS cybersecurity through Purdue Enterprise Reference Architecture (PERA) [4], renowned for its comprehensive approach. PERA's distinctiveness lies in its lack of a gateway component, challenging conventional norms in critical infrastructure. This absence leads to a nuanced examination of network isolation strategies in ICS. While considering the Industrial Demilitarized Zone (IDMZ), its inapplicability due to the absence of a gateway is acknowledged. Consequently, our research underscores the need to enhance security by introducing NIDSs between the first and third layers of the PERA. Integrating PERA into intrusion detection improves understanding, optimizes deployment, and strengthens resilience against inappropriate network behaviors in industrial settings.

2.2. Network-Based Intrusion Detection System

Network-Based Intrusion Detection Systems (NIDS) are indispensable for cybersecurity, providing vigilant monitoring and timely alerts against potential intrusions in network traffic. The deployment of intrusion detection in ICSs, where network isolation is prevalent, poses a significant challenge. This study investigates the viability of integrating Snort, an open-source Intrusion Detection System, with tailored Operational Technology (OT) rules for such environments. Our methodology seamlessly incorporates Snort into ICSs, effectively addressing the complexities introduced by network isolation. Operating on signature and rule-based matching, Snort adeptly identifies abnormal network traffic and potential threats, solidifying its role as a reliable NIDS tool for ICSs in network-isolated environments. This integration significantly enhances cybersecurity by enabling the detection and response to potential intrusions within the constraints of network isolation.

2.3. Internal ICS Attack Scenarios

This study explores NIDSs deployment in Industrial Control Systems (ICS) within network-isolated environments. Our investigation identifies vulnerabilities, particularly in instances of command injection and IDE access attacks [5], posing risks to the confidentiality, integrity, and availability of ICS.

Examining NIDS deployment in ICS reveals internal attack methodologies. The TWISC@NCKU collaboration establishes a secure gateway control system testing platform at the third layer, emphasizing the critical role of sensor readings on Human-Machine Interface (HMI) in dam operations. Our research introduces cross-layer attack methodologies tailored to dam operations, disrupting sensor readings through Modbus/TCP packet injections to Programmable Logic Controllers (PLCs). Focusing on countering malicious shutdowns, specifically targeting PLC controllers, we develop security measures and IDSs to fortify ICS against evolving threats in complex network environments. This study offers practical solutions to enhance ICSs' security.

3. ICS Network Intrusion Detection Methods

To explore the deployment of NIDS in ICS, we developed a comprehensive framework encompassing SNORT deployment, PLC, NIDS, and HMI establishment. Initially, we utilized Twido to construct an HMI, offering monitoring and control for the PLC (TWDLCAE40DRF). To simulate an attack, we deliberately shutdown the controllers of PLC and employed Wireshark to capture Modbus packets. Subsequently, SNORT was implemented with a focus on configuring it as a NIDS.

NIDS is intended to be deployed at the third layer, specifically in the operational management segment, with the database at its core storing information displayed on the HMI. In this scenario, the objective of NIDS is to monitor the operational management layer of ICS to detect potential intrusion threats.

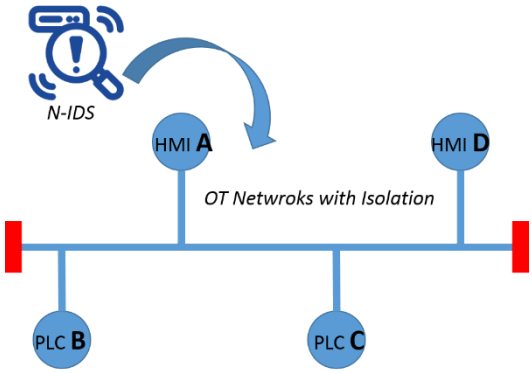

Fig. 1. NIDS, PLC, HMI Integration Architecture

During the integration of PLC and NIDS, we ensured seamless communication and monitored PLC communication to identify anomalies, with a particular emphasis on effectively detecting abnormal network behavior in an isolated network environment (Fig. 1). This comprehensive experimental procedure aims to assess the effectiveness of SNORT in ICS, contributing

to an improved understanding of cybersecurity enhancement in network-isolated environments.

In the pursuit of validating our proposed approach, we leverage the OT testbed provided by TWISC@NCKU. This cybersecurity testbed, specifically designed for dam control systems, serves as the foundation for our experiments. Its realistic representation of industrial control scenarios enables a practical examination of SNORT's deployment within a network-isolated environment.

Our investigation extends to the formulation of NIDS rules, particularly focusing on the integration of SNORT with tailored OT rules. The development of rules aims to detect attack techniques, with a special emphasis on countering malicious shutdowns, specifically targeting PLC controllers [6] (Fig. 2). This strategic development of rules contributes to fortifying ICS against evolving threats, thereby enhancing overall system security.

```
alert tcp any any -> any 502
(msg:"Detected Modbus/TCP Packet with
Data '41ff00'"; 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

In the experimental phase, we meticulously configured simulation parameters and established the experimental environment, focusing on realistic attack scenarios targeting Programmable Logic Controllers (PLCs). We simulated a shutdown attack on the controllers of PLC, capturing Modbus packets using Wireshark. Snort was configured as a NIDS with specific OT rules [7]. All experiments were conducted in the realistic dam control system testbed provided by TWISC@NCKU at National Cheng Kung University in Taiwan, ensuring authentic and reliable results. The configuration aimed to evaluate Snort's deployment effectiveness in industrial control systems with network isolation.

Utilizing the established experimental environment, a total of 30 experiments were conducted, each lasting 20 minutes and involving 0 to 20 instances of attacks. The attacks followed the methodologies outlined in Section 2.3. Background traffic, consisting of normal HMI [8] and PLC communication, was present in the environment (Fig. 3). The results indicated that, with an average of 4560 experimental packets, approximately 6.5 attacks were detected, resulting in a detection rate of 99.4%. The lowest detection rate, around 83%, occurred when interference devices were activated. In conclusion, there is a 99.4% probability of detecting attack packets, demonstrating the robustness of the proposed approach.

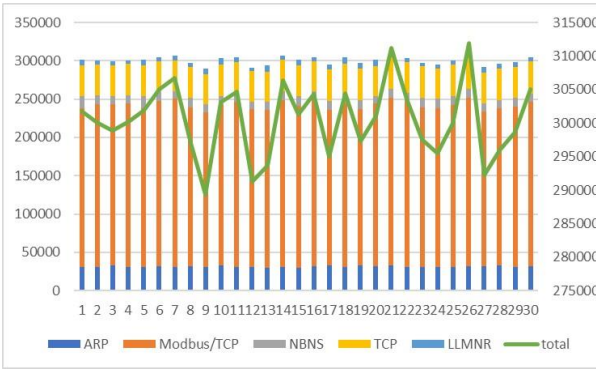

Fig. 3. Background Traffic in the Environment

5. Conclusion

This study delves into the deployment of NIDS, with a specific focus on Snort, in network-isolated ICS. Traditional intrusion detection systems often face challenges in ICS scenarios with network isolation, where they typically operate at gateway ports. Leveraging the cybersecurity testbed for dam control systems at TWISC@NCKU in Taiwan, our research validates Snort's efficacy in detecting abnormal network traffic, addressing the common issue of insufficient monitoring in network-isolated environments.

In the pursuit of enhancing the overall security of network-isolated ICS, this study emphasizes the necessity of adapting intrusion detection strategies to the unique challenges posed by critical infrastructure. Looking ahead, future research aims to broaden the scope by exploring additional attack scenarios. Due to current limitations in experimental settings, there are plans to incorporate Engineering Working Station (EWS) and introduce common IT attack scenarios to assess their effectiveness. This expansion will provide a more comprehensive understanding of the capabilities and limitations of intrusion detection systems in safeguarding network-isolated ICS against a diverse range of cyber threats.

Acknowledgements

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

References

1. E. Abdulova and A. Kalashnikov, “Categorization and Criticality Assessment of Facilities of Critical Infrastructure,” 2022 15th International Conference

Management of large-scale system development (MLSD), Moscow, Russian, 26-28 Sep. 2022.
2. P. Hu, B. Yang, D. Wang, Q. Wang, K. Meng, Y. Wang and Z. Chen, "Research on Cybersecurity Strategy and Key Technology of the Wind Farms' Industrial Control System," 2021 IEEE International Conference on Electrical Engineering and Mechatronics Technology (ICEEMT), Qingdao, China, 02-04 July 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. 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, Vol. 8, No. 1, pp. 29-32.
6. 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.
7. 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.
8. P. Papcun, E. Kajati and J. Koziorek, "Human Machine Interface in Concept of Industry 4.0," 2018 World Symposium on Digital Intelligence for Systems and Machines (DISA), 23-25 August 2018.

Authors Introduction

Ms. Nai-Yu Chen

She is a postgraduate of Cloud and Network Security (CANS) Lab, Institute of Computer and Communication Engineering, 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 Cloud and Network Security (CANS) Lab, Institute of Computer and Communication Engineering, 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.

Prof. 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.

Prof. 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, Wireless Network, Group Communication, and Reliable Transmission. He is the deputy director of Taiwan Information Security Center @ National Cheng Kung University(TWISC@NCKU).