VFAST Transactions on Software Engineering
http://vfast.org/journals/index.php/VTSE@ 2022, ISSN(e):2309-3978, ISSN(p): 2411-6246
Volume 10, Number 3, July-September 2022 *pp:37-42*

Industrial Control and Building Automation System Penetrating Testing using Modbus TCP Testbed

Muhammad Usman Ali, Muhammad Akhtar, Hanif Durad
Department of Computer and Information Sciences (DCIS), Pakistan Institute Engineering and Applied Sciences (PIEAS), Islamabad, Pakistan
Corresponding author email: hanif@pieas.edu.pk

ABSTRACT

Industrial Control System (ICS) plays a vital role in industries as it controls industrial processes such as power plants, food production, transportation, water and gas distribution etc. Similarly Building Automation System (BAS) is utilized for control, energy efficiency and conservation of modern buildings. As both BAS and ICS systems are becoming increasingly interconnected with networking technologies and becoming a lucrative target for attacks thus pose a serious threat to the infrastructure they control. ICS and BAS networks have been using legacy protocols with implementation of ICT protocols and technologies to be connected with modern networks. Thus, they have lack of security implementation. This paper presented a test-bed for testing vulnerabilities in Modbus protocol on HVAC control system. Two MITM attack scenarios were discussed and performed to demonstrate the weakness in the Modbus TCP protocol. The proposed system was tested using EasyIO-FS-32 server class controller having Modbus RTU, TCP and BACnet MSTP, TCP.

KEYWORDS

Industrial Control System, Building Automation System, Modbus TCP, Man-in-The-middle, SCADA, Cyber Security, Fuzzer, Penetration Testing

JOURNAL INFO

HISTORY: Received: August 8, 2022 Accepted: September 25, 2022 Published: September 30, 2022

INTRODUCTION

Industrial Control Systems (ICS) play a key role in providing many essential services to the society such as power generation, food industry, water treatment, oil & gas distribution, manufacturing and industrial process control. Traditionally, these systems existed in isolation from the Internet, but businesses intelligence required to track and manage their industrial networks by leveraging commercial networks instead of developing dedicated ICS networks for best vision of their production, supply chain system. Although this approach is cost effective, but it has exposed these systems to many threats. These systems were made using legacy equipment and protocols that are modified to operate on routable networks. These systems have been designed with simplicity and reliability without adequate safety criteria in mind and designed to work in isolation. Traditional isolation can't meet the security requirements of ICS. It is a big challenge to protect ICS systems from internal and external malicious attacks. Fan Xiaohe et al. investigated and reviewed traditional ICS. They analyzed characteristics of current ICS systems and also summarized the key security issues [1].

Moreover, the operational life span of ICS systems is above 20 years, so these systems have many unpatched vulnerabilities. Tools capable of conducting vulnerability testing can be especially useful to test the performance of the system before it is added to the manufacturing plant. One solution is the adaption of IT (Information Technolog) testing tools in ICS domain [2].

A typical ICS system consists of a master device one or more field deices and a communication network. ICS systems may consist of small number of devices connected to a controller to a complex network of interconnected devices extended over thousands of square kilometers. These controllers receive various information from sensors connected to physical systems, measure and monitor process variables like temperature, pressure and humidity to state of control valves. Based on these process variables ICS systems sends commands to control different field devices and get alerts from various components [3].

ICS consists of variety of systems i.e., Supervisory Control Systems (SCADA), Distributed Control Systems (DCS) and Programmable Logic Controllers (PLCs) [4]. Usually, SCADA systems are used to control facilities spread over thousands of miles. The central command and control system is necessary for these assets to function normally. SCADA systems provide central monitoring and control of field devices based upon alarms and status of these field devices. DCS are the control architecture systems for a plant consisting of several control loops that are spread across the system. Process control is usually done by implementing feedback or feed-forward control loop. To set the process in a desired set point PLCs are deployed which use combination of proportional, integral, and derivative control system. PLCs are small, embedded devices used to control specific process. PLCs are primary component of industrial process control and are commonly deployed in industries. With the advancement in development of

information technology, the demand for connection of ICS to other networks like internet is increasing day-by-day. Being not tailored with security these ICS and BAS devices connected to other networks is causing exposure to security threats. Researchers and industrialists are working on various measuring and managing approaches to implement security in ICS. They are following standards, guidelines and practices provided by industries standardization and governing bodies for ICS security [5]. NIST (National Institute of Standards and Technology) is an institute and standardizing body, they have released cyber security Framework guideline for ICS [2].

RELATED WORK

In this section we will discuss the prominent efforts made by researcher in the area fuzzing attacks on the ICS protocols particularly Modbus. The Modbus documentation clearly mentioned the unavailability of any kind of security features in this protocol. The researcher based on their experimentation proposed various security addenda to secure Modbus protocol in this era of cyber warfare.

Irfan et al. [16] developed a testbed to simulate near to actual SCADA facility as used for gas pipelines, water treatment plants and power grids. The setup is built with physical elements but on smaller scales with devices actually installed at Oil, gas fields and pipelines. The Modbus communication among the devices is simulated particularly. Attacks were performed to monitor the behavior the testbed performance.

There are many incidents that showed weakness in ICS systems [6], [7], [8] [17] and [18]. Any downtime or infiltration of ICS systems has enormous impact on thousands of users and may even result in a national disaster.

Modbus is the most commonly used communication protocol in ICS and BAS [9]. It lacks proper authentication and authorization mechanism. Researchers have investigated and proposed different solutions to produce confidentiality and authentication in modified Modbus protocol [10]. HMI is the overview of the whole plant to the operator, attack on HMI can result in loss of view (LOV) and in worst case manipulation of view (MOV) [11]. These devices are connected by communication medium which can be serial lines, Ethernet links, cellular networks and various types of radio signals. In 2021, Conti M et al. [9] provided a comprehensive survey of ICS. The also focused on architecture, employed devices, used protocols, testbeds and ICS datasets. They also categorized testbeds as Physical, Virtual, or Hybrid and they also discussed the current challenges of ICS [9].

In the perspective of cyber security, fuzzing could help in finding bugs in software, hardware and systems. Fuzzing method unexpected input is used to monitoring the behavior of device. V. J. M. Mans et al. discuss survey of fuzzing literature and design decisions made at every stage that make a fuzzer effective [12]. A state-of-the-art in fuzzing is published [13].

There are various types of security threats that are used by hackers for any malicious activity in any security system. Man-in-the-middle (MITM) is one of the most famous attack in ICS. MITM is a type of eavesdropping attack, where attackers interrupt an existing communication as ”middle” and pretended to be both participants. It allow the attacker in middle to manipulate the communication and intercept confidential information without knowing either of the two participants. Lan, Haiyan, et al. [14], proposed a method to classify traffic data to detect MITM attack in ICS. The experimental setup consisted of communication between SCADA system and Siemens S7- 300 series PLC. The attacker attacked using software named Ettercap through ARP poisoning. They provided simulations to classify the traffic data and calculated the accuracy up to 99.7%. In [15], Eigner O et al. proposed a machine learning based approach, they used k-Nearest Neighbors algorithm to define a valid/normal behavior model and then MITM was launched and compared the version during attack with normal behavior model and difference is calculated. At the end this approach was recognized as MITM detection system.

Table 1. Comparison of related works

Reference	Experimental setup	Protocol	Relevance	Primary Purpose
Irfan et al. [16]	Simulation	Modbus TCP	yes	Testing SCADA testbed
Mauro Conti et al. [9]	Survey	All ICS Protocols	yes	Survey of all legacy protocol
Roberto Nardone Et al. [10]	Modeling and simulation	Modbus	yes	Modeling of Modbus security
JIAPING MEN [11]	Simulation/ actual devices	Modbus	yes	Fuzzing the HMI of SCADA system
Valentin [12]	Modeling of Fuzzer	Not specific	yes	Utilization of Fuzzing technique
Honglian g Liang [13]	Survey	Not specific	yes	Understanding of fuzzing
Haiyan Lan [14]	PLC, SCADA softwar e	Siemens PLC	yes	Trafic classification for detection of MITM attack

Oliver Eigner et al. [15]	PLC HMI	Siemens PLC	yes	Detection of MITM attack on ICS
Parian et al [17]	Simulation	Modbus TCP	yes	Exploiting weaknesses in Modbus
Luswata et al. [18]	Simulation	Modbus TCP	yes	Pen testing of modbus protocol

LIMITATIONS

A number of researchers did experiments for the analysis of security posture of ICS and BAS protocols. In the above section several papers were studied but most of them used simulated environment for their experimentation as mentioned below.

In [16] simulation testbed used to perform attacks. In [9] and [10] formal security survey and assessment were performed. A classification of traffic data was done to assess the type of MITM attack in [14].

Machine learning approach was used in detecting the difference of behavior during MITM attack by [15]. Only LOV was performed in [11] for IOT device.

In this paper an experimental setup is performed using the industry most utilized hardware in ICS and BAS system along with operational HVAC system and sensor. Fuzzing technique is used for finding security loop wholes in Modbus protocol.

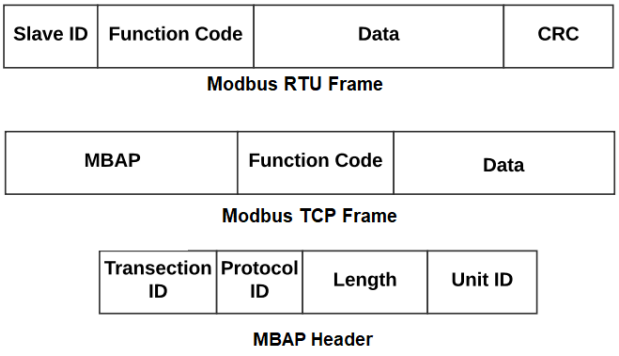

Figure 1. Modbus RTU frame format

A. Modbus Frame Format

Modbus RTU (Remote Terminal Unit) was originally designed as non-routable protocol to work on serial bus. Modbus TCP (Transmission Control Protocol) is Modbus RTU encapsulated in TCP/IP frame. Modbus RTU frame is comprised of address, function code, data and error check. Modbus TCP frame consists of Modbus Application (MBAP) Header, function code and data. Figure 1 shows the Modbus TCP and RTU frames.

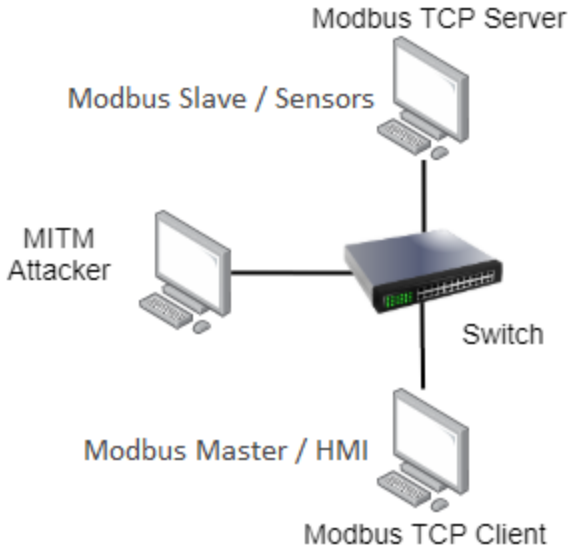

Figure 2. Modbus TCP MITM attack testbed architecture

METHODOLOGY

Need for a real time study was felt on physical operational HVAC system, control by a control system having both Modbus TCP and RTU variant. In this study we have utilized fuzzing techniques to monitor the effect of MITM attack on the system. Testbed proposed in this paper consist of a Modbus TCP client which also acts as HMI and Modbus Sensor. HVAC system was setup to read the temperature and humidity readings and based on these readings it controls the HVAC system. Master device sends query to the sensor and sensor responds with the reading. MITM attack was performed using Ettercap tool in kali linux.

EXPERIMENTAL SETUP

Figure 2 shows penetration testing using MITM attack tested-bed architecture. The testbed comprised of a Modbus TCP server (Master station), a Modbus TCP client (slave) connected through switch and a MITM attacker. EasyIO-FS-32 controller was used as Modbus master. Master station is connected to Heating, Ventilation, and Air Conditioning (HVAC) control system.

Attacker can launch man-in the middle attack on Modbus protocol to intercept network traffic between Modbus master and slave. Moreover, attacker can send false information to the master and slave by changing the contents of Modbus request and response. Attacker performs ARP poisoning attack and place itself between two devices communicating using Modbus TCP protocol. One device act as Modbus TCP Master and Other device acts as Modbus TCP Slave device. In this scenario EasyIO FS-32 controller act as Modbus Master device and Modbus Sensor as Slave device. It also acts as HMI and displays the sensor readings and current state of the devices it operates to the user. All the devices are connected to Local Area Network (LAN)

using network switch. Modbus Master device gets sensor data from Modbus sensor and based sensor readings it makes decisions to operate physical devices such as heating, ventilation and air conditioning.

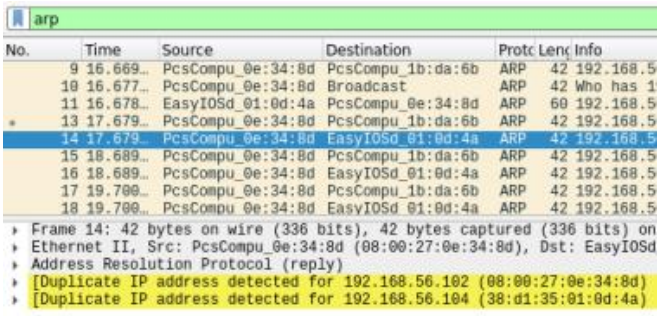

Figure 3. ARP spoofing attack in Wireshark

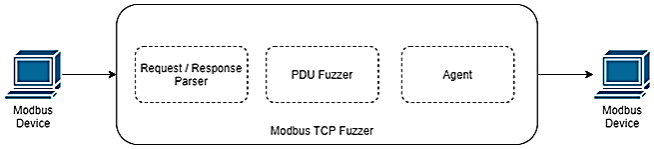

Figure 4. Components of Modbus TCP Fuzzer

A. Scenario 1: ARP Spoofing

Address resolution protocol (ARP) is used for address resolution of network layer address (IP address) to Datalink layer address (MAC Address). In order to get the MAC address of the destination host, source host broadcasts the ARP request to LAN and destination host with that IP address replies with the MAC address of the destination host. The source host then caches the IP and MAC pair to its local ARP cache in order to avoid the need to broadcast again. In ARP spoofing attack, attacker sends falsified ARP packets to victims once attacker's MAC address is associated with victim's IP address, attacker starts receiving traffic meant for the victim as shown in Figure 4.

In this attack attacker could intercept the Modbus query and sensor readings. In this case sensor values were not visible on HMI causing Loss of View (LOV). Attacker could also intercept the Modbus commands to operate an actuator causing Loss of Control (LOC). In next scenario attacker intercepted the query and sent the modified query to the sensor and caused Manipulation of Control(MOC). Moreover, attacker changed the sensor reading and sent the false readings to HMI causing Manipulation of View (MOV).

B. Scenario 2: Fuzzer

Modbus fuzzer was placed between master and slave device communicating using Modbus TCP protocol. In this scenario EasyIO FS-32 controller acted as Modbus Master device and Modbus Sensor as Slave device. All the devices were connected using LAN. Fuzzer is comprised of three components, request parser, PDU fuzzer and agent.

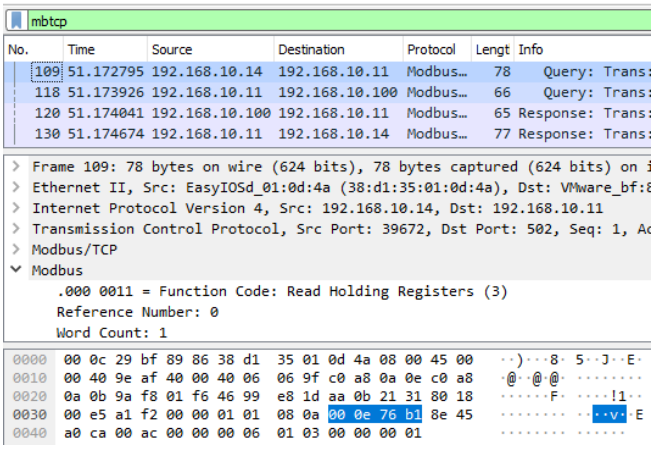

Figure 5. Wireshark snippet for no fuzzing communication across master and sensor

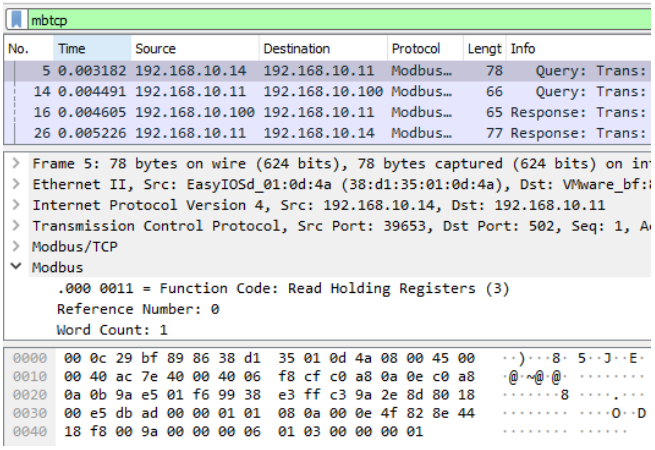

Figure 6. Wireshark snippet for request fuzzing communication across master and sensor

1) **Request Parser:**
Request parser consists of a request Modbus server which captures handles incoming requests from the master and extract PDU and MBAP headers from the request. Modbus protocol fields such as Function code, starting address and number of addresses are passed to Modbus fuzzer.
2) **PDU Fuzzer:**
PDU fuzzer uses the Information passed by request handler to generate new request with address or data field fuzzed.
3) **Agent:**
Agent consists of a Modbus client. Its function is to pass the new fuzzed request to the sensor and get the response from the sensor. Received response is then fuzzed and passed to the master device.

Master was setup to control the HVAC system based on the sensor readings. Fuzzer could operate in no fuzzing, request fuzzing and response fuzzing mode.

- **No fuzzing:**

In this mode, fuzzer passed the request without modifying it. Master requested the sensor readings and received the corresponding readings in response. Figure 5 shows the normal communication between master and sensor without fuzzing.

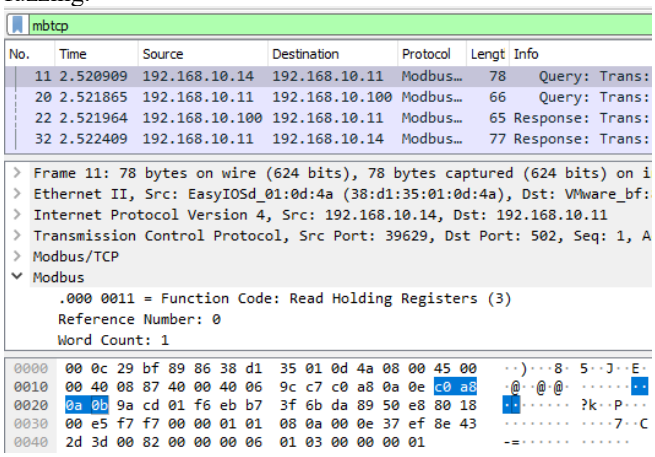

Figure 7. Wireshark snippet for response fuzzing communication across master and sensor

- **Request fuzzing:**

Modbus request was captured and relayed to the recipient after fuzzing its address field which result is manipulation of control. Master device sent the request to read the sensor data stored the holding registers of the Modbus/TCP sensor. Request Parser captured the request and extracted PDU and MBAP header from the request. It then performed the fuzzing on address field present in PDU. A new request was generated by packing fuzzed PDU and MBAP previously extracted from the request. This was done by PDU fuzzer. Agent then sent the request to client device which was a sensor in this case and waited for the response. When response arrived, it forwarded the response back to the HMI which displayed the wrong values on the screen and issued control commands to field devices based on the false data received from the sensor. Figure 6 shows the request fuzzing between master and sensor.

- **Response fuzzing:**

During response fuzzing response of a Modbus request was captured and relayed to the HMI essentially resulting manipulation of view. Master device sent the request to read sensor data. This request was captured by the request parser and forwarded to the sensor unchanged by agent. PDU fuzzer fuzzes the response with false value and sends back to the Master device displayed the false values on HMI and performed decision on wrong sensor data. Figure 7 shows the response fuzzing between master and sensor.

RESULT AND DISCUSSION

In this paper, a MITM attack was performed to manipulate the senor values and control the commands issued by the master controller. The experimental setup in this paper was comprised of EasyIO-FS-32 controller and HVAC system. The paper also proposed architecture for Modbus TCP fuzzer. Fuzzing was used to test the robustness of a cyber-physical system. This paper also demonstrated testbed for MITM attacks, in which two scenarios were exhibited. In ARP spoofing, attacker was successful in placing itself between master and slave and successfully manipulated the requests and responses. In Modbus fuzzer, the requests and responses were fuzzed to display the manipulated sensor values to HMI and caused the LOV, LOC, MOV and MOC.

CONCLUSION:

ICS and BAS systems are of great importance in our modern society. Traditionally these systems were designed with efficiency and reliability in mind without proper consideration for security. It is the need of the hour to secure these systems from different cyber-attacks. This paper investigates the cyber security vulnerabilities in ICS and proposed a testbed for MITM attacks on HVAC system. ARP spoofing and fuzzing based MITM attacks were used to test the vulnerabilities in Modbus TCP protocol. This paper demonstrated weakness in the Modbus protocol by exploiting the lack of authentication in Modbus protocol and display manipulated values to the operator and perform wrong decision by the controller. Future work may include testing the vulnerabilities in other protocols used in ICS such as BACnet, DNP3, PROFIBUS and PROFINET.

CREDIT AUTHOR STATEMENT

Muhammad Usman Ali: Conceptualization, Methodology, Writing- Original draft preparation, Visualization **Muhammad Akhtar**: Investigation., Validation., Writing- Reviewing and Editing **Hanif Durad:** Supervision, Editing, Validation

COMPLIANCE WITH ETHICAL STANDARDS

It is declared that all authors don't have any conflict of interest. Furthermore, informed consent was obtained from all individual participants included in the study.

REFERENCES

[1] X. Fan, K. Fan, Y. Wang, and R. Zhou, "Overview of cyber-security of industrial control system," in 2015 international conference on cyber security of smart cities, industrial control system and communications (SSIC). IEEE, 2015, pp. 1–7.

[2] K. Stouffer, J. Falco, K. Scarfone et al., "Guide to industrial control systems (ics) security," NIST special publication, vol. 800, no. 82, pp. 16–16, 2011.

[3] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," vol. 89, p. 101677.

[4] T. Macaulay and B. L. Singer, Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS. CRC Press, 2011.

[5] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," International journal of critical infrastructure protection, vol. 9, pp. 52– 80, 2015.

[6] S. S. S. R. Depuru, L. Wang, V. Devabhaktuni, and N. Gudi, "Smart meters for power gridchallenges, issues, advantages and status," in *2011 IEEE/PES Power Systems Conference and Exposition*. IEEE, 2011, pp. 1–7.

[7] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," vol. 5, no. 6, p. 29.

[8] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," vol. 1, no. 4, pp. 33–39.

[9] M. Conti, D. Donadel, and F. Turrin, "A survey on industrial control system testbeds and datasets for security research," *arXiv preprint arXiv:2102.05631*, 2021.

[10] R. Nardone, R. J. Rodrguez, and S. Marrone, "Formal security assessment of modbus protocol," in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2016, pp. 142– 147.

[11] J. Men, G. Xu, Z. Han, Z. Sun, X. Zhou, W. Lian, and X. Cheng,"Finding sands in the eyes: vulnerabilities discovery in iot with eufuzzer on human machine interface," *IEEE Access*, vol. 7, pp. 103 751–103 759, 2019.

[12] V. Manes, H. Han, and C. Han, "sang cha, manuel egele, edward schwartz, and maverick woo. 2019. the art," *Science, and Engineering of Fuzzing: A Survey. IEEE Transactions on Software Engineering PP (10 2019)*, pp. 1–1, 2019.

[13] H. Liang, X. Pei, X. Jia, W. Shen, and J. Zhang, "Fuzzing: State of the art," *IEEE Transactions on Reliability*, vol. 67, no. 3, pp. 1199–1218, 2018.

[14] H. Lan, X. Zhu, J. Sun, and S. Li, "Traffic data classification to detect man-in-the-middle attacks in industrial control system," in *2019 6th International Conference on Dependable Systems and Their Applications (DSA)*. IEEE, 2020, pp. 430–434.

[15] O. Eigner, P. Kreimel, and P. Tavolato, "Detection of man-in-the-middle attacks on industrial control networks," in *2016 International Conference on Software Security and Assurance (ICSSA)*. IEEE, 2016, pp. 64–69.

[16] Ahmed, I., Roussev, V., Johnson, W., Senthivel, S., Sudhakaran, S., 2016. A scada system testbed for cybersecurity and forensic research and pedagogy, in: Proceedings of the 2nd Annual Industrial Control System Security Workshop, ACM. pp. 1–9

[17] Parian, Christopher, Terry Guldimann, and Sajal Bhatia. "Fooling the master: Exploiting weaknesses in the Modbus protocol." Procedia Computer Science 171 (2020): 2453-2458.

[18] Luswata, John, Pavol Zavarsky, Bobby Swar, and Davison Zvabva. "Analysis of scada security using penetration testing: A case study on modbus tcp protocol." In 2018 29th Biennial Symposium on Communications (BSC), pp. 1-5. IEEE, 2018