2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)

Deep Packet Inspection in Industrial Automation Control System to Mitigate Attacks Exploiting Modbus/TCP Vulnerabilities

Osborn N. Nyasore
Information System Security and Assurance Management
Concordia University of Edmonton
Edmonton, Canada
onyasore@csa.concordia.ab.ca

Pavol Zavarsky
Information System Security and Assurance Management
Concordia University of Edmonton
Edmonton, Canada
pavol.zavarsky@concordia.ab.ca

Bobby Swar
Information System Security and Assurance Management
Concordia University of Edmonton
Edmonton, Canada
bobby.swar@concordia.ab.ca

Raphael Naiyeju
Information System Security and Assurance Management
Concordia University of Edmonton
Edmonton, Canada
rnaiyeju@csa.concordia.ab.ca

Shubham Dabra
Information System Security and Assurance Management
Concordia University of Edmonton
Edmonton, Canada
sdabra@csa.concordia.ab.ca

***Abstract*—Modbus TCP/IP protocol is a commonly used protocol in industrial automation control systems, systems responsible for sensitive operations such as gas turbine operation and refinery control. The protocol was designed decades ago with no security features in mind. Denial of service attack and malicious parameter command injection are examples of attacks that can exploit vulnerabilities in industrial control systems that use Modbus/TCP protocol. This paper discusses and explores the use of intrusion detection and prevention systems (IDPS) with deep packet inspection (DPI) capabilities and DPI industrial firewalls that have capability to detect and stop highly specialized attacks hidden deep in the communication flow. The paper has the following objectives: (i) to develop signatures for IDPS for common attacks on Modbus/TCP based network architectures; (ii) to evaluate performance of three IDPS - Snort, Suricata and Bro – in detecting and preventing common attacks on Modbus/TCP based control systems; and (iii) to illustrate and emphasize that the IDPS and industrial firewalls with DPI capabilities are not preventing but only mitigating likelihood of exploitation of Modbus/TCP vulnerabilities in the industrial and automation control systems. The results presented in the paper illustrate that it might be challenging task to achieve requirements on real-time communication in some industrial and automation control systems in case the DPI is implemented because of the latency and jitter introduced by these IDPS and DPI industrial firewall.**

Keywords—industrial control and automation system security, Modbus/TCP, deep packet inspection, intrusion detection and prevention system, industrial firewall

I. Introduction

DPI used by industrial firewalls is a form of packet filtering that locates, identifies, classifies, reroutes or blocks packets with specific data or code payloads that conventional packet filtering, which examines only packet headers, cannot detect [1]. DPI is an additional component of stateful filtering that goes beyond the communication header all the way to the payload. IDPS with DPI capabilities are able to use signatures to detect and mitigate likelihood of a successful attack on Modbus/TCP slave. Similar to IDPS, an industrial firewall can be used as a DPI tool. The firewall can be configured to utilize DPI rules to identify the content of Modbus messages and their sources and to drops all messages with control commands not authorized.

While commercial industrial firewalls have the DPI capabilities, the signatures for common attacks (such as different possible command injection attacks) on Modbus based network architectures are not available for open source IDPS [1]. This paper focuses on developing signatures for the common attacks and to use the signatures to evaluate performance of the three IDPS in detecting and preventing attacks in Modbus/TCP master – slave networks.

Implementation of the DPI reduces likelihood of exploitation of vulnerabilities in Modbus/TCP protocol. However, as shown in the paper, that the use of DPI can make it a challenge to meet requirements on latency and jitter in some real-time communication in industrial automation and control systems.

The paper also illustrates, by using the approach of the Common Vulnerability Scoring System (CVSS v3) [2], that expectations on the performance of DPI in reducing likelihood of exploitation of Modbus vulnerabilities in industrial system architectures should not be overestimated. As show in the paper, the DPI tools are capable of reducing the overall CVSS v3 vulnerability severity scores of Modbus based networks from “Critical / High” to “Medium”. In other words, the industrial automation and control systems that rely on the vulnerable Modbus/TCP remain vulnerable, to a lesser degree, despite the use of DPI capabilities of IDPS and industrial firewalls.

The paper is organized as follows. Related work is introduced in Section II. The testbed and performed experiments are explained in Section III of the paper. Results can be found in Section IV. Finally, Section V concludes the paper.

II. Related Work

The security of industrial control systems is in general designed to consider recommendations of the U.S. NIST SP 800-82 Rev.2 [3] and IEC/ANSI/ISA 62443 series of standards [4]. The IEC 62443 security standards introduces the concepts of zones, conduits, and security levels as security controls to restrict unnecessary flow of traffic

978-1-7281-6873-9/20/$31.00 ©2020 IEEE

DOI 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00051

between zones of different trust level. It is emphasized in [5] that firewalls with DPI capabilities for filtering industrial control protocols are indispensable elements in implementing important security principles, standards, and best practices of IEC 62443. While partitioning of an industrial control network and placement of multiple firewalls at various locations provides defense in-depth against cyber-attacks, it is important to consider the impact of these firewalls on nodes distributing time critical communications [6]. The firewall devices control and monitor traffic to and from zone. They are configured to pass only minimum traffic that is required for the correct system operation, blocking all other unnecessary traffic.

IDS that perform real-time deep inspection of Modbus/TCP packets is presented in [7]. The intrusion detection system uses a rule extraction model with parsers at the network, transport and application layers. While the network layer parser extracts from the packet information such as the source and destination IP address, the transport layer parser extracts information like source and destination ports and sequence number. The application layer parser extracts the application layer information necessary for analysis of the content of the packets, such as Modbus function code and reference number. IDPS used in our experiments described in Section III provide similar DPI capabilities.

The response time is a critical performance factor in some industrial and automation control systems. An interesting comparison of performance of three industrial firewalls can be found in [9]. The results of research on performance of open source network intrusion detection systems – Snort, Suricata and Bro - are documented in [8]. The results presented in Section IV of this paper are extending the results for DPI on industrial networks.

An approach to perform real-time deep inspection for Modbus TCP traffic by a rule extraction and deep inspection is proposed in [7]. The rule extraction module analyzes characteristics of industrial traffic and explores the relationship among the key fields in the Modbus TCP protocol. The deep inspection module is based on rule-based anomaly intrusion detection. According to [9], the proposed approach provides a very low false positive rate in detection of a malicious traffic.

The use of implicit denying firewalls is advocated in [10]. The argument is made that industrial control networks are designed to implement whitelisting in processing of packets that allows only whitelisted packets to pass through the firewall. The paper also explores how the number and complexity of firewall rules affect the performance of a firewall. Increase of the number of firewall rules introduces delays in the network. The relative position of the firewall rules affects the performance on the network. The effect on the performance on industrial application firewall depends on the amount of traffic flow in the network is analyzed in [11],[12]. Elimination of anomalies in the firewall and the IDPS is critical to the performance of industrial network. Work in [11] worked on a design of a firewall basing their effort on anomaly elimination and first verifying of firewall rules. Anomaly such as shadowing, correlation, generalization and redundancy can raise problem to a firewall or an IDS.

Modbus/TCP was not designed with security features in mind. Therefore, mitigating attacks exploiting Modbus/TCP is an important step in protecting the industrial control system. Vulnerabilities of Modbus/TCP have been illustrated by [13] using penetration testing tools. The use of SMOD and Metasploit framework are used in the research to extend of the work in [13]. The work illustrated the use of a fuzzer tool to pinpoint the weakness in each Modbus implementation. The tool sends a range of correct and malformed packet to target and record the response for later analysis. With the help of IDS, alerts are generated to show such attacks. The firewall will then be configured to block such packets in the network.

Identifying vulnerabilities in Modbus/TCP is Imperative to industrial control system. This help in building a resilience network when using Modbus/TCP. The work presented [14] describes the use of fuzzing technique to identify vulnerabilities in Modbus protocol. By knowing the vulnerabilities in Modbus/TCP, secure measures can be taken to prevent industrial control system from attacks. Using fuzzing tool MTF, various bugs were identified that led to denial of service attack or crushing of the system due to malformed packets in the network. In [15] the same tool is used. To collect information from the memory operating in three faces- reconnaissance phase, fuzz testing phase and failure detection phase.

The work in this paper tries to explore and validate that the use of Modbus/TCP is a vulnerable protocol that was not designed with security features in mind and can lead to cyber-attacks. Therefore, the use of defence in depth mechanism such as IDPS and firewall tries to mitigate these attacks reducing the risk level e.g. from high to medium protecting critical industrial control systems. In the result and finding of this paper it shows that we can minimize the risk of cyber-attack thus protecting industrial control systems.

III. Experimental Setup

In industrial automation and control systems, communication latency is considered as a primary performance index, since the effectiveness of a control action may be deeply influenced by delays experienced by packets traversing firewalls and other filtering equipment [5].

The testbed used to perform experiments consists of the Master Terminal, Slave Terminals, Intrusion Detection System, firewall and an Attacker as shown in Fig. 1.

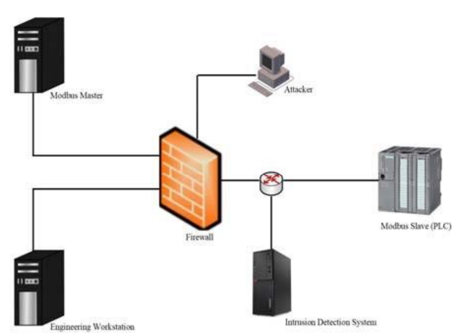

Fig. 1. Testbed architecture for development of attack signatures for IDPS and for study of impacts of deep packet inspection IDPS on latency in real-time industrial applications.

Modbus master is used to collect information from Slave units and sending out commands. In this testbed, Modbus master is simulated using open-source QModMaster tool.

Engineering workstation is used to send and receive read commands from the Modbus slave (PLC). Engineering worskstation is simulated using QModMaster tool.

Modbus slave receives the control information from the master. It also pushes the status of different sensors to the master, when requested. In this testbed, ModbusPal is used to simulate slave devices.

In this testbed, the attacker's activities are simulated by the Metasploit framework and by the SMOD Modbus penetration testing framework to perform attacks on integrity and availability of Modbus slave devices. The SMOD modules used in the experiments are summarized in table 1.

TABLE I. SMOD MODULE USED IN THE EXPERIMENT

Offensive Modules
Modbus/function/readSingleCoil
Modbus/function/readSingleRegister
Modbus/function/writeSingleCoil
Modbus/function/writeSingleRegister
Modbus/dos/writeSingleCoil
Modbus/dos/writeSingleCoil
Modbus/scanner/ScanUid

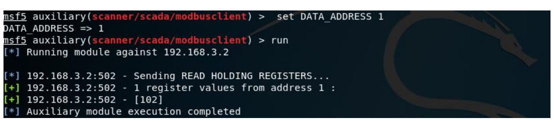

Fig. 2. Example of metasploit module used in the experiment

IDPS with DPI capabilities - Snort, Suricata, and Bro - are set up using Security Onion. Theses IDPSs monitor any incoming traffic to slave devices.

DPI firewall rules are configured utilizing iptables that provide a dynamic inspection feature called u32 match. The firewall conducts a DPI of traffic allowing or blocking traffic as defined by the firewall rules. The u32 match directs the extraction of 32 bits from the message at any specific location and performs a comparison with a given value.

PingPlotter is used to measure network latency and packet loss between the Modbus Master and Slave caused by IDPS with DPI capabilities. The DPI signatures were developed for the common attacks that can be used for identification of vulnerabilities in the Modbus/TCP network implementations or to trigger DoS attacks, The developed signatures include signatures for invalid encapsulated interface transport request and response parameters, illegal read file record response message parameters, invalid read and/or write multiple registers response parameters, invalid read and/or write coils/multiple coils request/response and read exception status parameters. The signature contains the protocol bytes that can confirm validity or invalidity of a given Modbus packet.

The tested IDPS were configured to use the developed signatures to check the Modbus/TCP function code and the request/response packet against the Modbus protocol specifications and to alert if the packet does not comply with the protocol

IV. RESULT AND FINDINGS

In this section some of the experimental results are discussed. Latency in the network caused by the DPI is presented. Modbus/TCP vulnerabilities are also discussed.

A. Impact of Deep Packet Inspection by IDPS on communication latency in Modbus/TCP networks

The experiment was performed to compare performance of three popular IDPS with DPI capabilities – Bro, Snort and Suricata. In the experiments, illegitimate requests were sent from the attacker's node to the Modbus slave. Attacks results of the three IDPS exploiting vulnerabilities listed in Table II below were performed while monitoring impacts of the intrusion detection systems on the communication latency. Typical PingPlotter results for the three tested IDPS are shown in Fig. 3, Fig. 4 and Fig. 5.

TABLE II. LATENCY OF IDPS WITH DEEP PACKET INSPECTION

IDPS	**Average Latency**	**Maximum Latency**
Bro	4.2ms	132ms
Snort	21.6ms	650 ms
Suricata	89.2ms	722 ms

In the experimental testbed, the average latency with the Bro IDPS was 4.2 ms, compared to 21.6 ms in Snort and 89.2 ms when using Suricata. The minimum value of the latency was also achieved by using Bro. The maximum latency was five-six times lower then when using Snort or Suricata

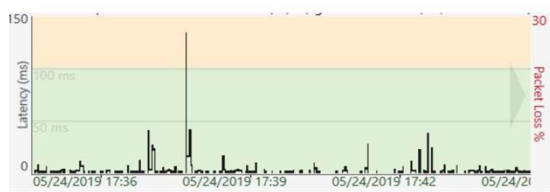

Fig. 3. Latency graph for Bro.

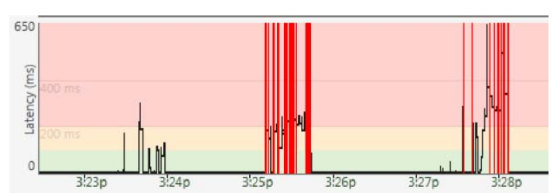

Fig. 4. . Latency Graph for Snort

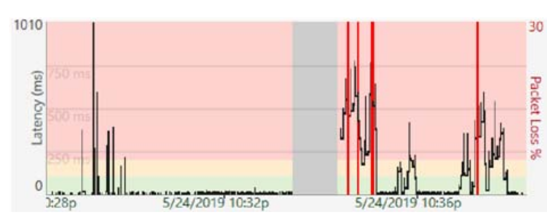

Fig. 5. Latency Graph for Suricata

B. *Vulnerability Assesment*

The Modbus/TCP vulnerabilities listed in Table III were evaluated using the Common Vulnerability Scoring System (CVSS) v.3.1 [2]. For each of the Modbus/TCP vulnerability the corresponding Base Score for a network architecture without IDPS was calculated. Then the Temporal and Environmental Scores were calculated for all selected vulnerabilities for network architectures with deep packet inspection protective measures implemented.

TABLE III. EXAMPLE OF EXPLOITABLE MODBUS/TCP VULNERABILITY AND POSSIBLE IMPACTS

Modbus/TCP Vulnerabilities
Confidentiality disclosure by unauthorized read coil request
Confidentiality disclosure by unauthorized read register request
Integrity compromise by unauthorized write register request
Integrity compromise by unauthorized write coil request
Availability compromise by DOS attack (multiple write)
Authentication bypass by scan UID request
Authentication bypass scan discover request

In the attack that exploits the large data overflow vulnerability, Modbus packets are repeatedly sent changing multiple values in the slave device with random values. The CVSS v.3.1 Base Score for the Modbus/TCP vulnerability is shown in Table IV. The base score for the vulnerability has the quantitative value "Critical". As shown in Table IV, implementation of operational environment security measures of the DPI by the intrusion detection provides the overall vulnerability score of 6.9 of the quantitative value "Medium". Note that the implemented environmental security measure of DPI to reduce likelihood of exploitation of vulnerabilities in Modbus/TCP is not sufficient to reduce the CVSS overall score to a "Low (0.1-3.9)" value.

TABLE IV. LARGE DATA OVERFLOW

Large Data Overflow CVSS v.3.1 Overall Score = 6.9 (Medium)	
CVSS Base Score = 9.4 (Critical)	**Metric Value**
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	High
Availability	High
CVSS Temporal Score = 8.9 (High)	
Exploit Code Maturity	Functional
Remediation Level	Workaround
Report Confidence	Confirmed
CVSS Environmental Score = 6.9 (Medium)	
Confidentiality Requirement	Low
Integrity Requirement	High
Availability Requirement	High
Modified Attack Vector	Local
Modified Attack Complexity	Low
Modified Privileges Required	Low
Modified User Interaction	Required
Modified Scope	Unchanged
Modified Confidentiality	Low
Modified Integrity	High
Modified Availability	High

During the attack, snort rules were configured to capture malicious traffic. Attack was detected due to the identified vulnerabilities in Modbus/TCP. Squert was able to show the alerts as shown in the figure 6 below. The protocol identifier, length of the query packet and function code are used here to detect suspicious content that was detected by Intrusion detection system.

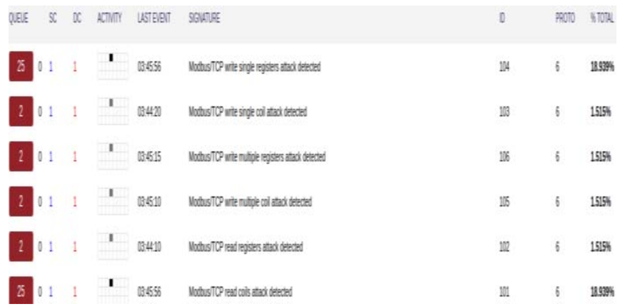

Fig. 6. Captured Alerts Displayed by Squert.

During the attack, wireshark was used to capture the traffic from the attacker to the Modbus Slave (PLC). Both Smod tool and Metasploit framework were used to query packets to the Modbus Slave.

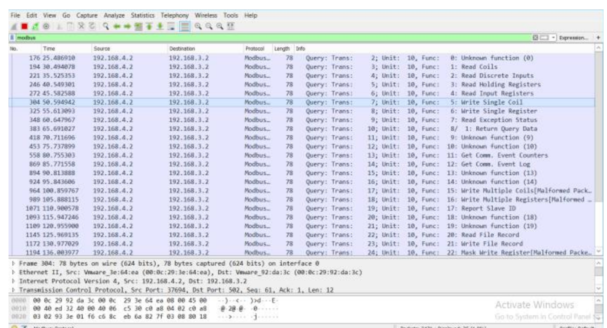

Fig. 7. Traffic Captured by Wireshark.

V. CONCLUSION

In the paper, the DPI was considered as a security measure to reduce likelihood of having Modbus/TCP vulnerabilities exploited in industrial automation and control system implementations. Considering that the Modbus/TCP can be used in applications requiring close to real-time communication latency, one of the objectives of the paper was to report on the results of performance evaluation of three popular intrusion detection systems – Bro, Snort and Suricata – in detection of possible attacks exploiting Modbus/TCP vulnerabilities. The results of the experiments show that it might be a challenging task to meet latency requirements on real time communication in Modbus/TCP systems that are under attack and protected by tools with DPI capabilities. Moreover, it is shown in the paper, by using the Common Vulnerability Scoring System CVSS v.3.1, that while the DPI tools are capable to reduce the likelihood of exploitation of Modbus/TCP vulnerabilities, the tools alone are not sufficient to reduce the overall CVSS score to a low level.

REFERENCES

[1] J. Nivethan and M. Papa, "On the use of open-source firewalls in SCADA systems", in Information Security Journal: A Global Perspective, 2016

[2] FIRST Common Vulnerability Scoring System (CVSS) v3.1: Specification document, June 2019, Available: https://www.first.org/cvss/v3.1/specification-document

[3] NIST Special Publication 800-82 Revision 2, Guide to industrial control systems (IACS) security, May 2015 Available:

[4] https://doi.org/10.6028/NIST.SP.800-82r2

[5] ANSI/ISA 62443-3-3: 2013 Security for industrial automation and control systems: System security requirements and security levels, 2013.

[6] Davison Zvabva, Pavol Zavarsky, Sergey Butakov, John Luswata, "Evaluation of industrial firewall performance issues in automation and control networks", 29th IEEE Biennial Symposium on Communications (BSC 2018), Ryerson University, Toronto, Canada, June 6-9, 2018.

[7] W. Yusheng, F. Kefeng, L. Yingxu, L. Zenghui, Z. Ruikang, Y. Xiangzhen, L. Lin, "Intrusion Detection of Industrial Control System based on Modbus TCP Protocol", 2017 IEEE 13th Int. Symposium on Autonomous Decentralized Systems (ISADS 2017), Bangkok, Thailand, March 22-24, 2017

[8] M.Cereia, I.Cibrario Bertolotti, L.Durante, A.Valenzano "Latency Evaluation of a Firewall for Industrial Networks Based on the Tofino Industrial Security Solution". Proceedings of the IEEE Emergency Technology and Factory Automation(ETFA) 2014

[9] J. Tafto Rodfoss, "Comparison of Open Source network Intrusion Detection Systems", University of Oslo, Department of Informatics May, 2011

[10] Y. Xu, Y. Yang, T. Li, J. Ju, Q. Wang, "Review on Cyber Vulnerabilities of Communication Protocols in Industrial Control Systems" State Grid Jiangsu Electric Power Research Institute, Nanjing, China. Nov. 2017

[11] S. Khummanee, A.Khumseela, S.Puangpronpitag, "Towards a New Design of Firewall: Anomaly Elimination and Fast Verifying of Firewall Rules", 10th International Joint Conference on Computer Science and Software Engineering (JCSSE), 2013.

[12] M.Cheminod, L.Durante , L.Seno , A.Valenzano , "Performance Evaluation and Modeling of an Industrial Application-Layer Firewall" IEEE Transactions on Industrial Informatics, Volume: 14 , Issue: 5 , May 2018.

[13] M. Sabraoui, J.L. Hieb, J. H. Graham ,"MODBUS Protocol Fuzzing for Cyber Security and Hardening of Industrial Control Systems", https://www.researchgate.net/publication/290732323

[14] A. G. Voyiatzis, K. Katsigiannis, S. KoubiasA; "Modbus/TCP Fuzzer for Testing Internetworked Industrial Systems" University of Patras, GR-26504, Patras, Greece, May 2015

[15] K. Katsigiannis, D. Serpanos; "MTF-Storm: a high performance fuzzer for Modbus/TCP", Dept. of Electrical & Computer Engineering University of Patras Patras, Greece. 2018

[16] Modbus Application Protocol Specification Available online http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf

[17] Snort Manual Organisation retrieved from http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node11.html#SECTION00295100000000000000

[18] Metasploit. (2019). Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit. [online] Available at https://www.metasploit.com/

[19] Modbus Poll tool. Available: http://www.modbustools.com/

[20] ModbusPal slave simulator tool. Available at: https://sourceforge.net